

COMPUTING WITH COLOURED TANGLES

AVISHY Y. CARMİ AND DANIEL MOSKOVICH

ABSTRACT. We suggest a diagrammatic model of computation based on an axiom of distributivity. A diagram of a decorated coloured tangle, similar to those that appear in low dimensional topology, plays the role of a circuit diagram. Equivalent diagrams represent bisimilar computations. We prove that our model of computation is Turing complete, and with bounded resources that it can decide any language in complexity class IP, sometimes with better performance parameters than corresponding classical protocols.

1. INTRODUCTION

The present research represents a step in a programme whose goal is to study topological aspects of information and computation. Time is a metric notion, and so any such topological aspects would presumably have no internal notion of time. We consider a notion of computation which is independent of time and which is natively formulated in terms of information. We construct a diagrammatic calculus whose elements we call *tangle machines*. These were first defined in [16]. A key feature of tangle machines is that they come equipped with a natural notion of *equivalence* which originates in the beautiful diagrammatic algebra of low dimensional topology. Tangle machines serve in this paper as abstract flowcharts of information in computation. We prove that the computational paradigm that we propose contains Turing Machines and Interactive Proofs (thus it does not ‘lose anything’), and it also contains additional models (*e.g.* Section 8.1).

The world we observe around us evolves along a time axis, so a tangle machine could not be used as a blueprint for a classical computer. Time is a more nebulous concept in the quantum realm, however, and it might be that tangle machine constructions are relevant for adiabatic quantum computations or in other quantum contexts [16]. In particular, they naturally incorporate the axiom of uniform no-cloning (Remark 5 in Section 4.1). The main relevance of our work would probably be to isolate and access natively topological aspects of classical and quantum computation. We also speculate that tangle machine computations can emerge physically via dynamical processes on a tangle machine, given a set of input colours, and that perhaps something like this actually occurs in nature. After all, natural computers are not Turing machines.

How might tangle machines manifest themselves in nature? The authors make the following speculation. Evolutionary biology provides an analogue to tangle machines in the notions of phenotype versus genotype [17, 26]. The external characteristics of an organism such as its appearance, physiology, morphology, as well as its behaviours are collectively known as a *phenotype*. The *genotype* on the other hand refers to the inherent and immutable information encoded in the genome. Two phenotypes may look entirely different but may nevertheless share the same genotype. Could information about an organism be encoded as a tangle machine, where equivalent machines represent different phenotypes which share the same genotype? Might the process of evolution of an organism be described by a series of basic transformations akin to the Reidemeister moves exerted

1991 *Mathematics Subject Classification.* 68Q05; 03D10; 57M25.

Key words and phrases. Diagrammatic algebra; Low dimensional topology; Computation; Turing machine; Interactive proof.

The authors thank M. Buliga and L.H. Kauffman for useful discussions that inspired the present note.

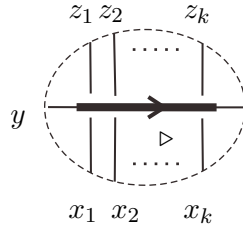


FIGURE 1. An interaction in a machine, where $z_i \stackrel{\text{def}}{=} x_i \triangleright y$ for $i = 1, 2, \dots, k$.

by the environment on the organism, which change its phenotype while preserving its genotype, along with occasional ‘violent’ local moves on a current configuration which change its genotype? Might tangle machines describe a way in which nature process its information primitives— its organisms?

There are two obvious advantages to a topological model of computation. The first is that it is very flexible by construction. Bisimilar computations (Definition 10) are represented by topologically equivalent objects, which are related in a simple way (Section 10). The second, which we do not discuss in this paper, is that we have a notion of *topological invariants* which are characteristic quantities which are intrinsic to a bisimilarity class of computations.

In the introduction we briefly introduce tangle machines in Section 1.1 after which we state our main results in Section 1.2 and give scientific context in Section 1.3.

1.1. What is a tangle machine computation? A tangle machine is built up out of *registers* each of which may hold an element of a set Q . The set Q comes equipped with a set B of binary operations representing basic computations. For $\triangleright \in B$, we read $x \triangleright y$ as ‘the result of running the programme $\triangleright y$ on input data x ’. An alternative evocative image is that $x \triangleright y$ is a ‘fusion of information x with information y using algorithm \triangleright ’. Our binary operations satisfy the following axioms which equip (Q, B) with what is called a *quandle* structure (see Section 3.2 for this and extensions):

Idempotence: $x \triangleright x = x$ for all $x \in Q$ and for all $\triangleright \in B$. Thus, x cannot concoct any new information from itself.

Reversibility: The map $\triangleright y: Q \rightarrow Q$, which maps each colour $x \in Q$ to a corresponding colour $x \triangleright y \in Q$, is a bijection for all $(y, \triangleright) \in (Q, B)$. In particular, if $x \triangleright y = z \triangleright y$ for some $x, y, z \in Q$ and for some $\triangleright \in B$, then $x = z$. Thus, the input x of a computation may uniquely be reconstructed from the output $x \triangleright y$ together with the programme $\triangleright y$.

Distributivity: For all $x, y, z \in Q$ and for all $\triangleright, \blacktriangleright \in B$:

$$(1) \quad (x \triangleright y) \blacktriangleright z = (x \blacktriangleright z) \triangleright (y \blacktriangleright z) .$$

This is the main property. It says that carrying out a computation $\blacktriangleright z$ on an output $x \triangleright y$ gives the same result as carrying out that computation both on the input x and also on the state y , and then combining these as $(x \blacktriangleright z) \triangleright (y \blacktriangleright z)$. In the context of information, this is a *No Double Counting* property [15].

Later in this paper, in Remark 5 in Section 4.1, we show that uniform *no-cloning* and *no-deleting*, which are fundamental properties of quantum information, follow from Reversibility and Distributivity for an appropriate colouring by a generalization of a quandle called a *quagma*. This observation argues for Reversibility and Distributivity as being nature’s most fundamental information symmetries.

The basic unit of computation in a tangle machine is an *interaction* representing multiple inputs x_1, \dots, x_k independently fed into a programme $\triangleright y$ as depicted in Figure 1. These are concatenated (perhaps also with wyes) to form a *tangle machine*— see Section 3.

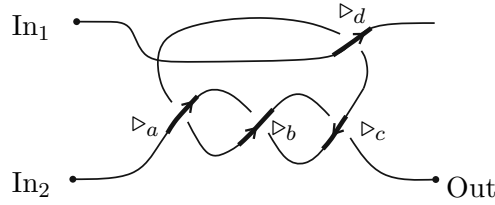


FIGURE 2. A sample computation. Determining colours for input registers In_1 and In_2 uniquely and instantaneously determines the colour for the output register Out .

A *tangle machine computation* begins with an initialization of a specified set of *input registers* to chosen colours in Q . A disjoint set of *output registers* is chosen. If the colours of the input registers uniquely determine colours for the output registers, then the colours of the output registers are the result of the computation. Otherwise the computation cannot take place. See Definition 6 and Figure 2). This provides a model of computation.

Remark 1. *More generally we may allow the result of the computation to be the (possibly empty) set of all possible colours out output registers. This level of generality is not required in this paper.*

A tangle machine computation has the following features:

- (1) Whereas the alphabet of a classical Turing machine is discrete (usually just 0 and 1 and maybe 2), the alphabet Q of a tangle machine can be any set, discrete or not. Two values of Q may be chosen to represent 0 and 1, while the rest may represent something else— perhaps electric signals.
- (2) Whereas a Turing machine computation is sequential with each step depending only on the state of the read/write head and on the scanned signal, a tangle machine computation is instantaneous and is dictated by an oracle. Time plays no role in a tangle machine computation.
- (3) A tangle machine computation may or many not be deterministic (colours may represent random variables and not their realizations), and it may or may not be bounded (contain a bounded number of interactions). Quandles and tangle machines are flexible enough to admit several different interpretations. In this paper, we use tangle machines to realize both logic gates (deterministic, composing into perhaps unbounded computations) and interactive proof computations (probabilistic, bounded size).
- (4) A tangle machine is flexible. There is a natural and intuitive set of local moves relating bisimilar tangle machine computations (Section 10).
- (5) A tangle machine representation is abstract. A tangle machine computation takes place on the level of information itself, with no reference to time. The axioms of a quandle have intrinsic interpretation in terms of preservation and non-redundancy of information.

1.2. Results. The purpose of this note is to show the following theorems:

Theorem 1. *Any binary Boolean function can be realized by a tangle machine computation.*

This is neither hard nor new— a previous such realization (not with tangle machines but with coloured braids) is recalled in Section 4.3.

By Turing completeness of the boolean circuit model, we have the following:

Corollary 2. *Tangle machines (with an unbounded number of interactions) are Turing complete.*

In Section 5 we further prove the following.

Theorem 3. *Any Turing machine can be simulated by a tangle machine. Such a tangle machine is coloured by a quandle (Q, B) whose set of binary operations B has cardinality $\mathcal{O}(n)$ where n is the number of states in the finite control of the underlying Turing machine.*

Tangle machines, whose notion of computation is based on an oracle which produced output colours from input colours, can in-fact perform super-Turing computations. See Remark 4.

Colours of registers in tangle machines evolve at *interactions*. If we bound the number of interactions, tangle machine computations include computations in a complexity class which we call TangIP which includes inside it a class which we call BraidIP. Letting χ denote the number of interactions in the machine, letting δ denote a ‘noise parameter’, and letting c and s denote *completeness* and *soundness* correspondingly (see Section 2.3), we have the following:

Theorem 4. $\text{IP} \subseteq \text{BraidIP} \{\delta, \chi\}$ where:

$$(2) \quad I(c\delta) < \chi < \frac{1}{I(1 - s\delta)},$$

with $I(p) \stackrel{\text{def}}{=} -p^{-1} \log p$. The growth rate of χ is $\mathcal{O}(\frac{1}{\delta})$ as $\delta \rightarrow 0$.

Thus, tangle machine computations with bounded interactions can decide any language in class IP, which is known to equal PSPACE [43].

Moreover, in the special setting of non-adaptive 3-bit probabilistically checkable proofs (PCP), there exists a tangle machine which achieves a better soundness parameter than the best known classical single-verifier non-adaptive 3-bit PCP algorithm (Section 9.1). Yet the soundness parameter for this tangle machine is above the conjectured lower limit. This suggests the possibility that tangle machines behave like very good single verifiers.

Finally, in Section 10, we discuss equivalence of machines. Machine equivalence formally parallels equivalence of tangled objects in low dimensional topology, and it gives us a formalism with which to discuss bisimulation. After justifying the definition, we introduce a notion of *zero knowledge* for machines, in which the proof is kept secure from untrusted verifiers at intermediate nodes.

Tangle machines are thus revealed to be a flexible model for computation.

1.3. Other low dimensional topological approaches to computation. The first person to consider distributivity as an axiom of primary importance, and to suggest diagrammatic calculi for logic (and perhaps by extension to computation) was American philosopher Charles Saunders Peirce. The following Peirce quotation was pointed out by Elhamdadi [19]: “These are other cases of the distributive principle... These formulae, which have hitherto escaped notice, are not without interest.” [40].

The idea to use diagrammatic calculi from low-dimensional topology to model computation was pioneered by Louis Kauffman, who used knot and tangle diagrams to study automata [28], nonstandard set theory, and lambda calculus [29, 14]. There is also a diagrammatic π calculus formulation of virtual tangles [35]. The diagrammatic calculus of braids (braids are a special class of tangles) also underlies topological quantum computing— see *e.g.* [31, 38]. Universal logic gates (Toffoli gates) have been realized using coloured braids [39, 33, 36]. This has led to a proposal for circuit obfuscation— masking the true purpose of a circuit— using braid equivalence [3]. Buliga has suggested to represent computations using a calculus of coloured tangles which is different from ours [13]. In another direction, a different diagrammatic calculus, originating in higher category theory, has been used in the theory of quantum information— see *e.g.* [2, 8, 46].

In our approach, the tangle diagrams themselves are computers, representing a flow-chart of information during a computation whose basic operations are distributive (compare [42]). This is not a diagrammatic lambda calculus or pi calculus, but rather it is a natively low dimensional topological approach to computation. In this note, we relate this approach to other approaches by showing that tangle machine computation is Turing complete, and in the bounded resource setting that it can decide any language in the complexity class IP.

1.4. Contents of this paper. We begin in Section 2 by recalling relevant models of computation such as Turing machines, IP, and PCP. Then, in Section 3, we recall the formalism of tangle machines [16]. Our definition is more general than the one used in that paper. Next in Section 4 we show that tangle machines are Turing complete, and we show in Section 5 how tangle machines may simulate Turing machines. Restricting to a bounded resources setting, we construct networks of deformed IP verifiers in Section 6, defining a complexity class BraidIP. In Section 7 we show that $\text{IP} \subseteq \text{BraidIP}$. Section 8 shows how to make our network computations more efficient by getting rid of the global time axis, making use of a machine we call the Hopf–Chernoff machine. Restricting further to a PCP proofs, in Section 9 we show that the Hopf–Chernoff machine gives us perfect completeness and a better soundness parameter than the best-known non-adaptive 3-bit PCP verifier. Finally, we define equivalence of machines in Section 10, where we also discuss the tangle machine analogue of a zero knowledge proof.

2. MODELS OF COMPUTATION

In this section, mainly to fix terminology and notation, we recall the notion of a Turing machine (Section 2.1), of decidable languages (Section 2.2), of interactive proof (Section 2.3), and of probabilistically checkable proof (Section 2.4).

2.1. Turing machines. The theory of computation and complexity theory are based on the notion of a *Turing machine* [45]. We recall its definition, following [24].

Definition 5. A Turing machine is a triple $(\Sigma, \mathcal{S}, \delta)$ where

- Σ is a finite set of symbols called the alphabet which contains a “blank” symbol.
- \mathcal{S} is a finite set of “machine states” with $q_0 \in \mathcal{S}$ and $q_h \in \mathcal{S}$ being, respectively, the initial and final (halting) states.
- $\delta: \mathcal{S} \times \Sigma \longrightarrow \mathcal{S} \times \Sigma \times \epsilon$ is a transition function.

The set $\epsilon = \{0, 1, 2\}$ indicates the movement of a tape (*Left*, *Stationary*, *Right*), or equivalently indicates the movement of a reading/writing (R/W) head following a writing operation. For convenience and without loss of generality, we limit the alphabet to three colours, $\Sigma = \{0, 1, 2\}$, where 2 represents the blank symbol.

A Turing machine is composed of two primary units. A *finite control unit* remembers the current state and determines the next state based on the current reading from a *memory unit*. The memory unit records symbols on a finite, possibly unbounded *tape*. Reading and writing operations retrieve or modify a symbol in the current position of the R/W head along the tape.

2.2. Computable functions and decidable languages. Computable functions are the basic objects of study in computability theory. In the context of Turing machines, a partial function $f: \Sigma^k \rightarrow \Sigma$ is *computable* if there exists a Turing machine that terminate on the input x (*input* means tape content) with the value $f(x)$ stored on the memory tape if $f(x)$ is defined, and which never terminates on input x if $f(x)$ is undefined.

A related notion is the notion of a decidable language. A set $L \subseteq \{0, 1\}^*$, called a *language*, is said to be *decided* by Turing machine M if there exists a computable function $f: \Sigma^k \rightarrow \Sigma$ satisfying $f(x) = 1$ if $x \in L$ and $f(x) = 0$ if $x \notin L$ for all $x \in \{0, 1\}^*$. A language is *decidable* if it is decided by some Turing machine.

2.3. Interactive proof. The *interactive proof* model of computation involves *bounded resources*, by which we mean that computations are constrained to make use of only a finite number of steps, polynomial in the length $|x|$ of the word $x \in \{0, 1\}^*$ [22]. Again, the goal is to determine whether $x \in L$ or $x \notin L$ for a language L . A *verifier* V interrogates a *prover* P who claims to have a proof that $x \in L$. Both the prover and the verifier are assumed to be honest and queries are assumed to be independent. We are given two parameters, *completeness* c and *soundness* s , with $c, s \in [0, 1]$. For the classical setting of **IP** we set $c = 2/3$ and $s = 1/3$. The verifier V believes that $x \in L$ at time t with probability V_t . This belief is updated each time P responds to a query, beginning from $V_0 = 0$. We say that the statement $x \in L$ is *decided at time* t if:

$$(3) \quad \begin{aligned} (\text{Completeness}) \quad & x \in L \longrightarrow \Pr(V_t = 1) \geq c; \\ (\text{Soundness}) \quad & x \notin L \longrightarrow \Pr(V_t = 1) \leq s. \end{aligned}$$

The class IP (Interactive Polynomial time) consists of those languages L that are decidable in time χ polynomial in $|x|$. A celebrated result in complexity theory states that IP equals PSPACE, the class of problems solvable by a Turing machine in polynomial space [43].

The class IP can be expanded to the class MIP in which the verifier has access to not one but many provers, which can be interrogated independently [11]. It has been shown that MIP equals the large class NEXPTIME [7].

2.4. Probabilistically checkable proofs. The class $\text{PCP}_{c,s}(r(|x|), q(|x|))$ is a restriction of IP in which the verifier is a polynomial-time Turing machine with access to $\mathcal{O}(r(|x|))$ uniformly random bits and the ability to query only $\mathcal{O}(q(|x|))$ bits of the proof, with completeness c and soundness s [6, 37]. The celebrated PCP Theorem states that $\text{PCP}[\mathcal{O}(\log |x|), \mathcal{O}(1)] = \text{NP}$ [5]. For PCP, the prover is thought of as an oracle. We restrict to the case of 3-bit PCP verifiers, *i.e.* to those for which $q(|x|) = 3$, and to those which are *non-adaptive*, *i.e.* for which verifier queries are independent of previous responses by the oracle.

The ideal PCP verifier would have $c = 1$ with minimal soundness s . A simple and good 3-bit PCP verifier with $s = \frac{3}{4} + \sigma \approx 0.75$ for arbitrarily small $\sigma > 0$ was designed by Håstad [23]. The current record is $s = \frac{20}{27} + \sigma \approx 0.741$ for an arbitrarily small $\sigma > 0$ [32]. It is conjectured that the lowest possible value of s is $\frac{5}{8} = 0.625$ [47].

3. TANGLE MACHINES

In this section we define tangle machines, first ignoring colours (Section 3.1) and then, after defining the sets we colour with (Section 3.2), then with colours (Section 3.3), where we also define tangle machine computations.

3.1. Without colours. We define here a *tangle machine*, without colours, to be a diagram which occurs by concatenating (connecting endpoints) of a finite number of *generators* of the form in Figure 3. Thickened lines in interactions (Figure 3b) are called *agents*, and each thin line is called *patients*. Only agents are directed, and there is no compatibility condition between directions of different agents.

Arcs in a tangle machine, ending as an under-arc passing under an agent or at a wye or at a machine endpoint (thus “continuing right through agents”), are called *registers*. Later on, registers will contain colours.

Tangle machines have struts and interactions as generators, whereas *trivalent tangle machines* have struts, interactions, and wyes as generators. An example of a machine constructed by concatenation is presented in Figure 4. As in the theories of virtual knots and of w-knotted objects, concatenation lines may intersect [9, 30]. Also, as in the theory

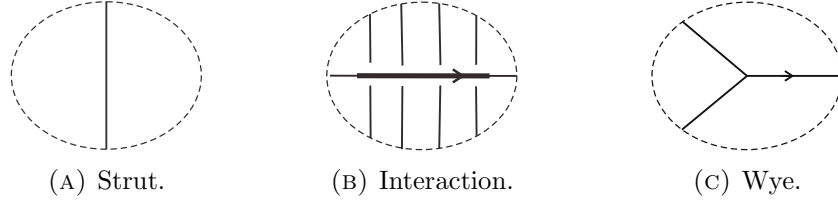


FIGURE 3. Generators for tangle machines are struts and interactions. Generators for trivalent tangle machines are struts, interactions, and wyes.

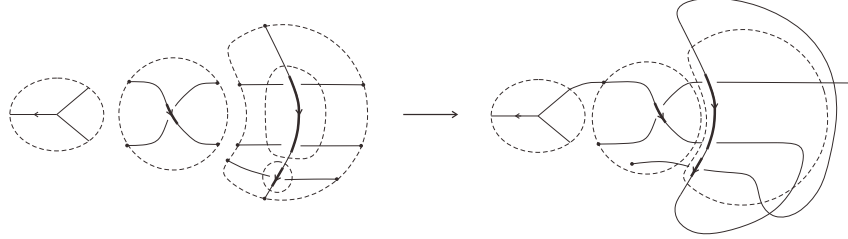


FIGURE 4. Concatenation of tangle machines.

of *disoriented tangles*, no compatibility condition is imposed for directions of concatenated agents [18].

3.2. Colours. Let Q be a set equipped with a family B of binary operations which satisfy the following three axioms:

Idempotence: $x \triangleright x = x$ for all $x \in Q$ and for all $\triangleright \in B$.

Reversibility: The map $\triangleright y: Q \rightarrow Q$, which maps each colour $x \in Q$ to a corresponding colour $x \triangleright y \in Q$, is a bijection for all $(y, \triangleright) \in (Q, B)$. In particular, if $x \triangleright y = z \triangleright y$ for some $x, y, z \in Q$ and for some $\triangleright \in B$, then $x = z$.

Distributivity: For all $x, y, z \in Q$ and for all $\triangleright \in B$:

$$(4) \quad (x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z) .$$

Remark 2. *Reversibility may be weakened by requiring only that $\triangleright y$ be an injection for all y , but not necessarily a surjection. This is indeed the case for the machines that we describe in the context of interactive proofs.*

The pair (Q, B) is called an *quagma*. It is called an *quandle* if the operations in B distribute over one another, in the sense that:

$$(5) \quad (x \triangleright y) \blacktriangleright z = (x \blacktriangleright z) \triangleright (y \blacktriangleright z) ,$$

for all $\triangleright, \blacktriangleright \in B$. This definition is a variant of definitions found in [12, 41, 25]. If we weaken reversibility to require only that $\triangleright y$ be an injection for all $y \in Q$ and for all $\triangleright \in B$, the resulting structure is called a *quandloid* [15]. Quagmas, quandloids, and quandles serve as the content of registers in tangle machines.

Example 1 (Conjugation quandle). *Colours might be elements of a group Γ , and the operation might be conjugation:*

$$(6) \quad x \blacktriangleright y = y^{-1}xy .$$

The pair $(\Gamma, \{\blacktriangleright\})$ is called a conjugation quandle. Such quandles feature in knot theory, e.g. [27].

Example 2 (Linear quandle). *Colours might real numbers and the operations might be convex combinations:*

$$(7) \quad x \triangleright_s y = (1 - s)x + sy \quad s \in \mathbb{R} \setminus \{1\} .$$

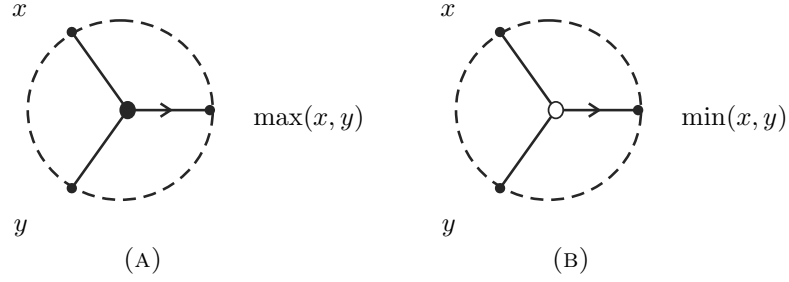


FIGURE 5. Colouring wyes coloured by max and min.

The pair $(Q, \{\triangleright_s\}_{s \in \mathbb{R}})$ is called a linear quandle.

3.3. With colours. A *colouring* of a tangle machine M is an assignment ϱ of a binary operation in B to each agent and an assignment ρ of an element of Q to each register, such that, at each interaction, the colour $z \in Q$ of the patient to the right of the agent (according to the right-hand rule) equals the colour of its corresponding patient to the left of the agent $x \in Q$ right-acted on by the colour of the agent $y \in Q$ via the operation of the agent $\triangleright \in B$:



Thus, an interaction ‘realizes’ the action of the quagma or of the quandle.

To colour a trivalent tangle machines, Q has to come equipped with a complete ordering. We include also an assignment of either max or min to each wye, so that the exiting register of the wye is the maximum of the two inputs if the wye is labeled max and is their minimum otherwise. We graphically denote a min label with a white circle at the branch-point of the wye, and a max label by a black circle. See Figure 5.

Remark 3. The notion of tangle machine given above is more general than in [15, 16], in which all tangle machines are quandle-coloured and without wyes.

Finally, we come to the notion of a tangle machine computation.

Definition 6. A computation of a (trivalent) tangle machine M is:

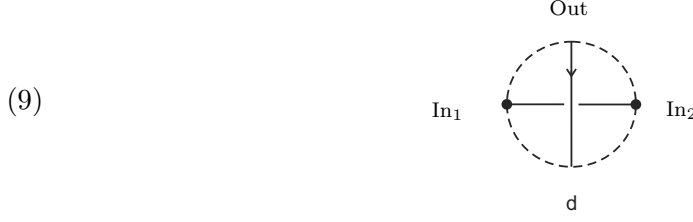
- (1) A choice of a set S_{in} of input registers in M .
- (2) A choice of a set S_{out} of output registers in M with $S_{in} \cap S_{out} = \emptyset$.
- (3) A colouring ϱ of all agents in M (and an assignment of either max or min to each wye).
- (4) A colouring ρ_{in} of all registers in S_{in} .
- (5) A unique (oracle) determination of a colouring ρ_{out} of all registers in S_{out} . If ρ_{in} does not uniquely determine ρ_{out} , the computation cannot take place.

4. TANGLE MACHINES ARE TURING COMPLETE

Our goal in this section is to realize the universal set of gates, NOT(\neg) and AND(\wedge), as well as a *multiplexer* which duplicates the content of a register, using tangle machines. This realizes the boolean circuit model, thus showing that tangle machines are Turing complete.

Remark 4. A tangle machine computation, which is based on an oracle which tells us the colours of output registers given colours of input registers, can carry out super-Turing computations. Consider the conjugation quandle of a group Γ with unsolvable conjugacy

problem, and colour agents In_1 and In_2 by elements of Γ . The colour of Out might not be Turing computable, but the tangle machine computation computes it.



4.1. **Quagma approach.** Choose the set of colours to be $Q \stackrel{\text{def}}{=} \mathbb{Q}^{2 \times 2}$, equipped with a set B of binary operations whose elements are the following:

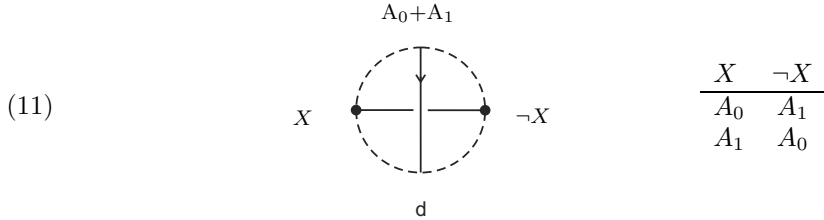
$$(10a) \quad X \blacktriangleright Y = \begin{cases} Y^{-1}XY, & \text{if } \det(Y) \neq 0; \\ X, & \text{otherwise.} \end{cases}$$

$$(10b) \quad X \triangleright_s Y = (1 - s)X + sY, \text{ for } s = \frac{1}{2} \text{ or } s = 2.$$

The structure $(Q, \{\triangleright_{0.5}, \triangleright_2, \blacktriangleright\})$, henceforth referred to simply as Q , is a quagma.

To realize boolean logic, let $A_0 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $A_1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ stand in for the digits 0 and 1 correspondingly. Incidentally, these happen to coincide with Pauli spin matrices of quantum mechanics.

A NOT gate is described by a single interaction



where the respective truth-table is shown to the right of the diagram. Explicitly,

$$(12) \quad \neg X = X \blacktriangleright (A_0 + A_1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} X \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The input is the register labeled X , the output is the register labeled $\neg X$, and the remaining register is always coloured by the constant value $A_0 + A_1$.

Realizing an AND gate can be split into several successive computations. Let X and Y be the inputs to the gate, and write $\mathbf{0}$ for $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. The following instructions end up with the desired operation $X \wedge Y$.

- (1) $\beta_1 = (A_0 + A_1) \blacktriangleright (X \triangleright_{0.5} Y) = (X + Y)^{-1}(A_0 + A_1)(X + Y)$
- (2) $\beta_2 = \beta_1 \triangleright_{0.5} (A_0 + A_1) = \frac{1}{2}\beta_1 + \frac{1}{2}(A_0 + A_1)$
- (3) $\beta_3 = (\beta_2 \triangleright A_0) \triangleright_{0.5} \beta_2 = \frac{1}{2}A_0\beta_2A_0 + \frac{1}{2}\beta_2$
- (4) $X \wedge Y = A_1 \blacktriangleright (\beta_3 \triangleright_{0.5} A_1) = (\beta_3 + A_1)^{-1}A_1(\beta_3 + A_1)$

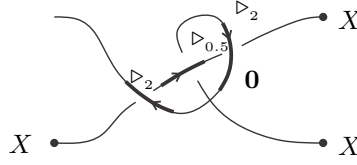
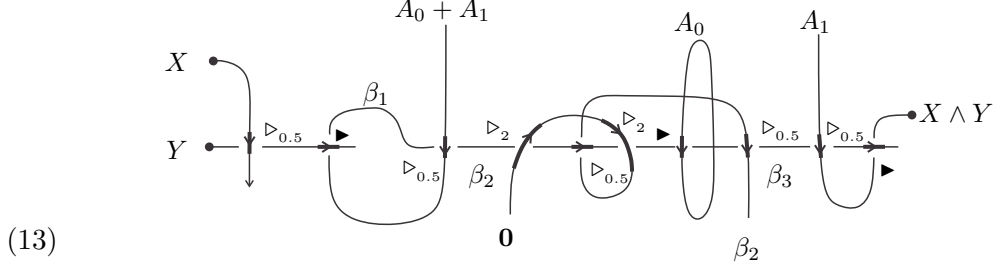


FIGURE 6. A multiplexer.

A tangle machine which realizes these steps is given below together with the respective truth-table.



(14)

X	Y	β_1	β_2	β_3	$X \wedge Y$
A_0	A_0	$A_0 - A_1$	A_0	A_0	A_0
A_0	A_1	$A_0 + A_1$	$A_0 + A_1$	A_0	A_0
A_1	A_0	$A_0 + A_1$	$A_0 + A_1$	A_0	A_0
A_1	A_1	$A_1 - A_0$	A_1	$\mathbf{0}$	A_1

In addition to the universal set of gates we also need to be able to duplicate the content of a register. The conventional boolean circuit model includes junction points along wires. The tangle machine analogue for such a junction is a *multiplexer*, that is a machine whose output colours are duplicates of the colour in one of its inputs. A multiplexer takes an input of the form $\{X, \underbrace{0, \dots, 0}_{n-1 \text{ times}}\}$, and outputs $\{X, \underbrace{\dots, X}_n\}$. The operation of a multiplexer is captured by the machine in Figure 6.

Remark 5. Two fundamental properties of quantum information are no-cloning and no-deleting. The uniform version of no-cloning states that there does not exist a unitary operator C for which $C(A \otimes e)C^\dagger = A \otimes A$ for all states A , where e denotes the identity operator. The uniform version of no-deleting states that there does not exist a unitary operator U for which $U(A \otimes A)U^\dagger = A \otimes e$ for all states A . Both of these statements are captured by the quagma axioms. Consider the quagma $(Q, \{\triangleright_{0.5}, \blacktriangleright\})$ where Q is the set of invertible operators and \blacktriangleright is any binary operation which distributes over $\triangleright_{0.5}$, e.g. conjugation. If U were a universal cloning operator with respect to \blacktriangleright , i.e. if $(A \otimes e) \blacktriangleright U = A \otimes A$ for all A , then for any state A both machines in Figure 7 would carry out the same computation and in particular $\text{Out}_1 = \text{Out}'_1$. But then $(A \triangleright_{0.5} B) \otimes (A \triangleright_{0.5} B) = \text{Out}_1 = \text{Out}'_1 = (A \otimes A) \triangleright_{0.5} (B \otimes B)$, which is false in general. Thus universal cloning violates distributivity. No-deleting follows from no-cloning because if U were a universal deleting operator with respect to \blacktriangleright then U would also be a universal cloning operator with respect its inverse operation \blacktriangleleft which exists thanks to reversibility. This would violate distributivity, because \blacktriangleleft also distributes over $\triangleright_{0.5}$ as can be seen by applying $\blacktriangleleft Z$ to both sides of the equation:

$$X \triangleright_{0.5} Y = \left((X \blacktriangleleft Z) \triangleright_{0.5} (Y \blacktriangleleft Z) \right) \blacktriangleright Z .$$

We parenthetically note that no-cloning and no-deleting are also captured by a different diagrammatic calculus, that of categorical quantum mechanics [1].

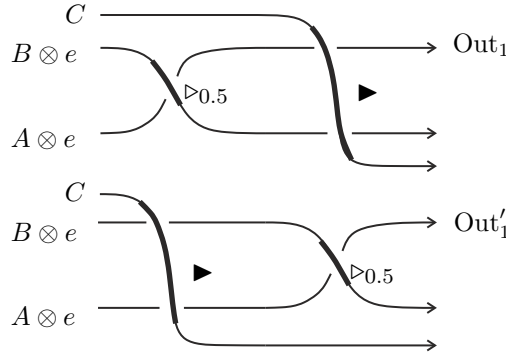


FIGURE 7. Universal cloning violates distributivity.

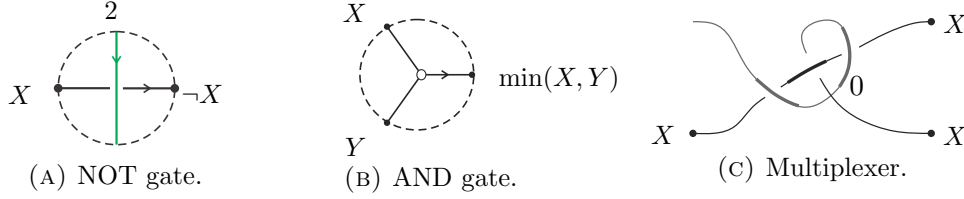


FIGURE 8. Logic gates for the 3-colour approach. Inputs are the colours on the left, and outputs are colours on the right.

4.2. Wye approach. Realizing a universal set of logic gates is easier if we allow wyes, and may be realized with a quandle colouring.

We colour our machines by elements of the quandle $Q \stackrel{\text{def}}{=} \{0, 1, 2\}$ subject to the quandle operation $x \triangleright y = 2y - x \pmod 3$ (this is a *Fox 3-colouring*). We totally order Q by $0 < 1 < 2$. Colour-code 0 as red, 1 as blue, and 2 as green. For this particular quandle the direction of the agent does not matter because the operation \triangleright is its own inverse. Let 0 stand in for the digit zero and 1 stand in for the digit one. A universal set of logic gates and a multiplexer can be obtained as in Figure 8, where an incoming arrow represents input and an outgoing arrow represents output.

4.3. Nonabelian simple group approach. The AND gate constructed in Section 4.1 was realized as a tangle machine coloured by a quagma which is not a quandle, and the AND gate of Section 4.2 used a wye. In fact, it is possible to realize a universal set of logic gates with a conjugation quandle coloured tangle machine without using wyes.

The construction is based on Barrington's Theorem [34, 10]. Following [36], Appendix A of [3] constructs a 132 crossing 14 strand braid coloured by the conjugation quandle of the finite simple group A_5 which realizes the Toffoli gate that is a universal logic gate [20]. This braid is made a tangle machine by interpreting each crossing as an interaction. Three of its registers are inputs, three are outputs, and it contains a number of *ancilla* which are what we called *control registers*.

5. TURING MACHINE SIMULATION

In this section, we show how to simulate a Turing machine using a tangle machine.

5.1. Turing tangle machine. In this section we make use of the linear quandle whose underlying set of elements Q is the set of the rational numbers and whose set of operations B is:

$$(15) \quad x \triangleright_s y = (1 - s)x + sy \quad s \in \mathbb{Q} \setminus \{1\} .$$

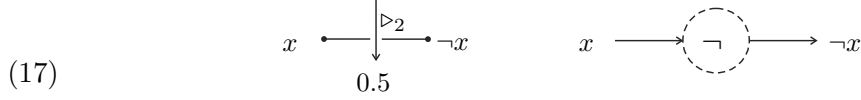
There are several sub-machines that recur in the construction of a *Turing tangle machine*, the tangle machine analog of a Turing machine. To simplify our diagrams we represent these sub-machines graphically.

Multiplexer: We indicate a multiplexer by splitting a strand.

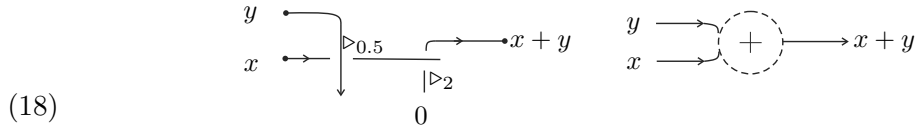


The multiplexer is realized by composing diagrams of the form in Figure 6.

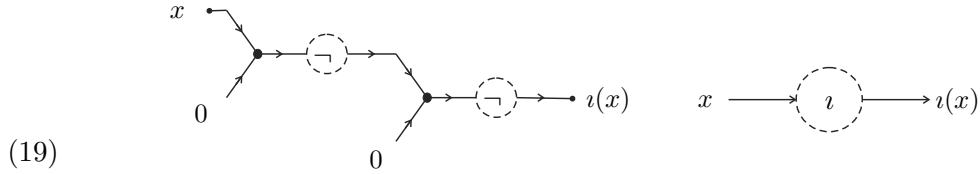
Negation: $\neg x \stackrel{\text{def}}{=} 1 - x$.



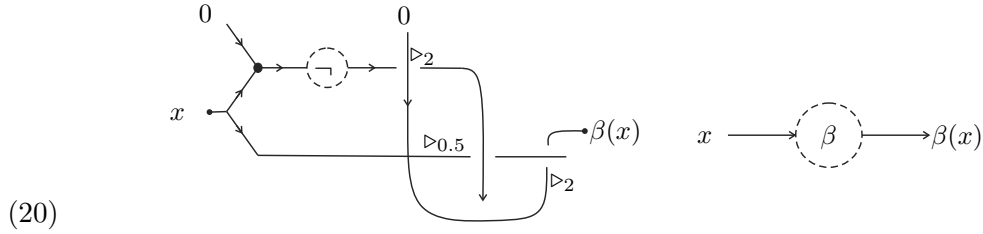
Addition:



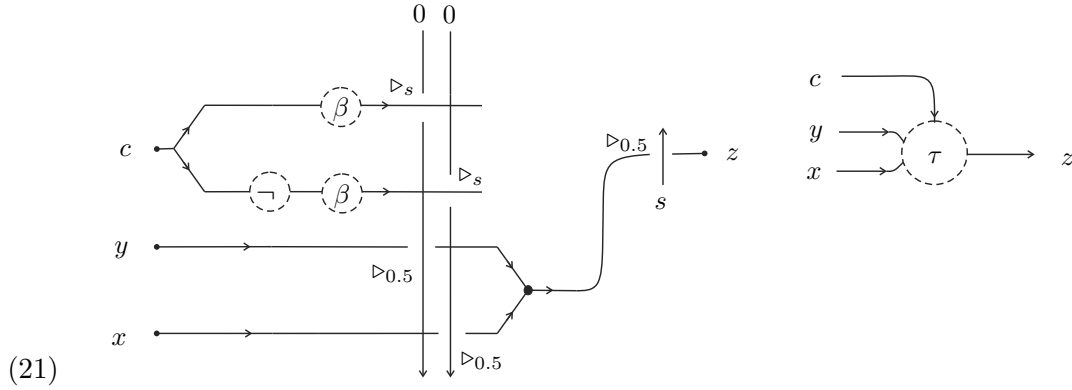
Indicator: If $x \geq 1$ then $\iota(x) = 1$, if $0 < x < 1$ then $\iota(x) = x$, otherwise $\iota(x) = 0$.



Beta: A function $\beta(x)$ which satisfies $\beta(0) = -1$, $\beta(\frac{1}{2}) = 0$, and $\beta(1) = 1$.



Selector: Depending on the colour c of a control strand, either x or y emerges as the output, z . To be precise, $z = x$ if $c = 0$ and $z = y$ if $c = 1$.



where s is an arbitrary constant whose value is greater than 2.

Mask generating machine: This sub-machine is shown in Figure 9. Its input registers are a register coloured by an integer $p \in Q$ called a *pointer*, and a sequence of coloured registers together called a *mask*. Its output registers are a register coloured p and one register coloured 0 for all other input coloured registers, except for a single register coloured 1 in the p th position of the output.

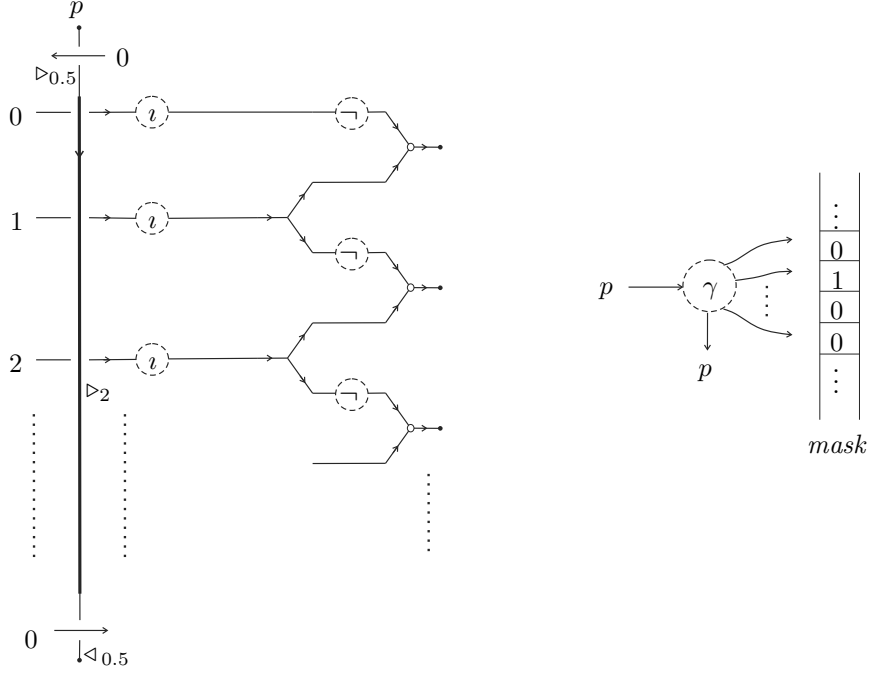


FIGURE 9. A mask generating machine.

5.2. Finite control. The first step in realizing a Turing machine is to mimic the finite control unit, *i.e.* to simulate the transition function

$$(22) \quad \delta(q(k), u(k)) = (q(k+1), a, \epsilon)$$

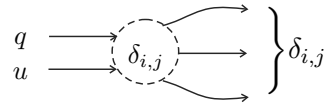
Given the *current machine state* $q(k)$ and the *symbol currently under the R/W head* $u(k)$, the *transition function* determines the *next machine state* $q(k+1)$ together with a pair of tape instructions: the *symbol to be written* a , and an ϵ movement of the head to its next position along the tape. Without loss of generality we shall assume henceforth that the finite control states are all natural numbers, and in particular that $\mathcal{S} = \{1, \dots, n\}$.

The basic building block of the finite control tangle machine is a *hardwired transition*, that is a function $\delta_{i,j} : \mathcal{S} \times \Sigma \rightarrow \mathbb{Z}^3$,

$$(23) \quad (q, u) \mapsto \begin{cases} (\bar{q} + 2, \bar{a} + 2, \bar{\epsilon} + 2), & \text{if } q = i \text{ and } u = j + 1; \\ (-\bar{q} - 2, -\bar{a} - 2, -\bar{\epsilon} - 2), & \text{otherwise.} \end{cases}$$

where $\bar{q}, \bar{a}, \bar{\epsilon}$ denote, respectively, the next assumed state and the tape instructions as specified in the definition of $\delta_{i,j}$. The parameters i, j and the respective output of $\delta_{i,j}$, the triplet $(\bar{q}, \bar{a}, \bar{\epsilon})$, are hardwired into the tangle machine realization of $\delta_{i,j}$ through the quandle parameters. See Figure 10.

The hardwired transition is symbolically represented as



The transition function δ is constructed by combining several hardwired transitions. Note that there are not more than $3n$ possible transitions in the finite control (n states

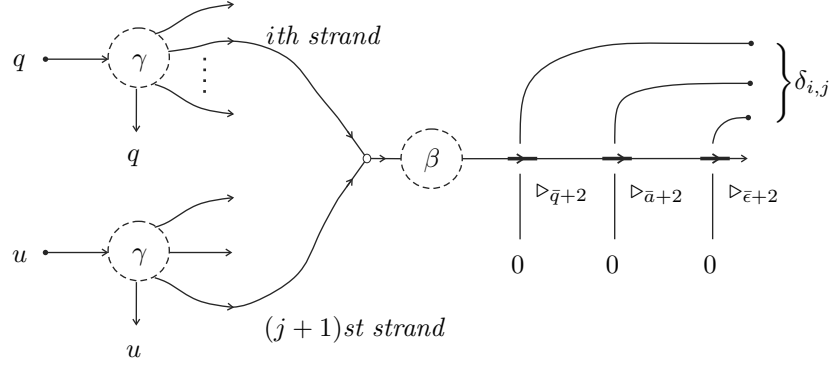


FIGURE 10. Hardwired transition.

multiplied by 3 input symbols). Thus the number of distinct binary operations in B does not exceed $9n + \mathcal{O}(1)$, which accounts for $3n$ triplets $(\triangleright_{\bar{q}+2}, \triangleright_{\bar{a}+2}, \triangleright_{\bar{\epsilon}+2})$ and a few other operations required for realizing the memory unit. A detailed construction of the finite control sub-machine is shown in Figure 11.

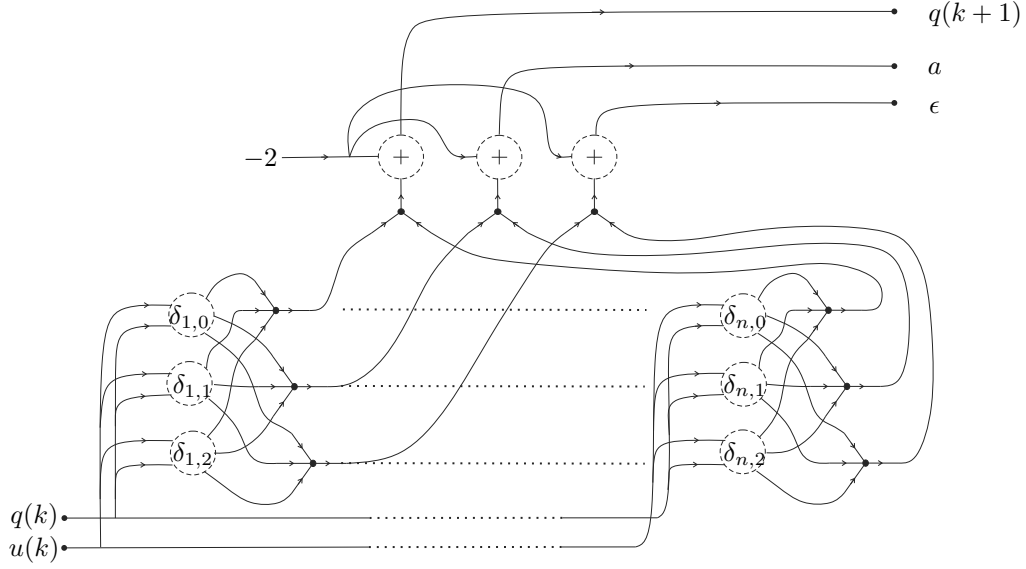


FIGURE 11. A tangle machine realization of a finite control unit.

5.3. Memory unit and one step computation. The memory unit consists mainly of the tape logic. It accepts a finite, possibly unbounded set of registers whose colours are manipulated in the basis of commands a and ϵ received from the finite control. The majority of the registers of the memory unit correspond to tape cells whose content is represented by colours from the set Σ .

We construct the memory (tape) reading and writing operations using a mask generating machine together with selector machines to output the colour of the $p(k)$ th register, either as it originally appeared or modified. See Figure 12.

Figure 13 illustrates the memory unit, connected to the finite control unit. Its inputs are:

- (1) An *integer pointer* register coloured $p(k)$, indicating the current head position.
- (2) A finite, possibly unbounded set of registers each of which represents a single (memory) cell on a tape. These tape registers are coloured $\{c_i(k)\}_{i>0} \in \Sigma$.
- (3) A pair of registers coloured correspondingly by a pair instructions (a, ϵ) , where a denotes the symbol to be written in the current cell to which the head points

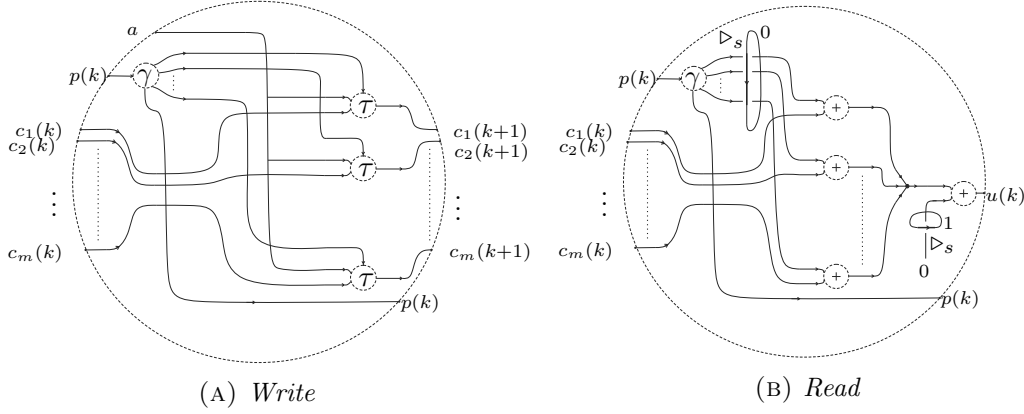


FIGURE 12. Memory reading and writing sub-machines. Here $\frac{1}{2} < s < 1$ is an arbitrary parameter.

(which is numbered $p(k)$), and ϵ denotes the (possibly zero) increment to be added to $p(k)$, so that $p(k+1) = p(k) + \epsilon - 1$.

The outputs of the memory unit are:

- (1) The updated pointer $p(k+1)$.
- (2) A finite, possibly unbounded set of registers whose colours $\{c_i(k+1)\}_{i \geq 0} \in \Sigma$ have been all passed unchanged, except for a single cell whose content may have been modified.
- (3) A strand coloured by $u(k+1)$, the content of the cell to which the head points in its new location $p(k+1)$

To simulate the sequential operation of a Turing machine, copies of the finite control unit and of the memory unit are to concatenated in the obvious manner. Concatenating N copies of the machine in Figure 13 simulates N successive computations of a Turing machine (see Figure 14). This justifies naming such a procedure *iteration*.

5.4. Halting. A halting state is a state for which:

$$(24) \quad \delta(q_h, u) = (q_h, u, 1)$$

Once arriving at a halting state, further iterations do not alter the memory content of the machine. The state q_h represents an equilibrium which may or may not be reached for a given input sequence $u(0), u(1), \dots$. A machine whose input registers are coloured by a halting state can be closed by concatenating respective inputs and outputs as shown in Figure 15.

6. INTERACTIVE PROOFS: DISTRIBUTION OF KNOWLEDGE BY DEFORMATION

The decision of a crowd can converge to a correct answer even when each individual has limited knowledge. This phenomenon is known as *wisdom of the crowds* [44]. In line with ‘the many being smarter than the few’, we extend the notion of interactive proof systems [22] to a system in which a collection of verifiers interact to prove a claim together. Might such a crowd of verifiers collaborate to prove more than could be proven by any individual verifier in the crowd?

6.1. Deformation of a single interaction. Consider a family of verifiers, each with a belief concerning whether $x \in L$ or $x \notin L$. We model the belief of each verifier W at time t as a Bernoulli random variable W_t whose realizations w_t are either |True) or |False). We interpret $w_t = |True)$ as ‘ W believes at time t that $x \in L$ ’, and we interpret $w_t = |False)$ as ‘ W believes at time t that $x \notin L$ ’.

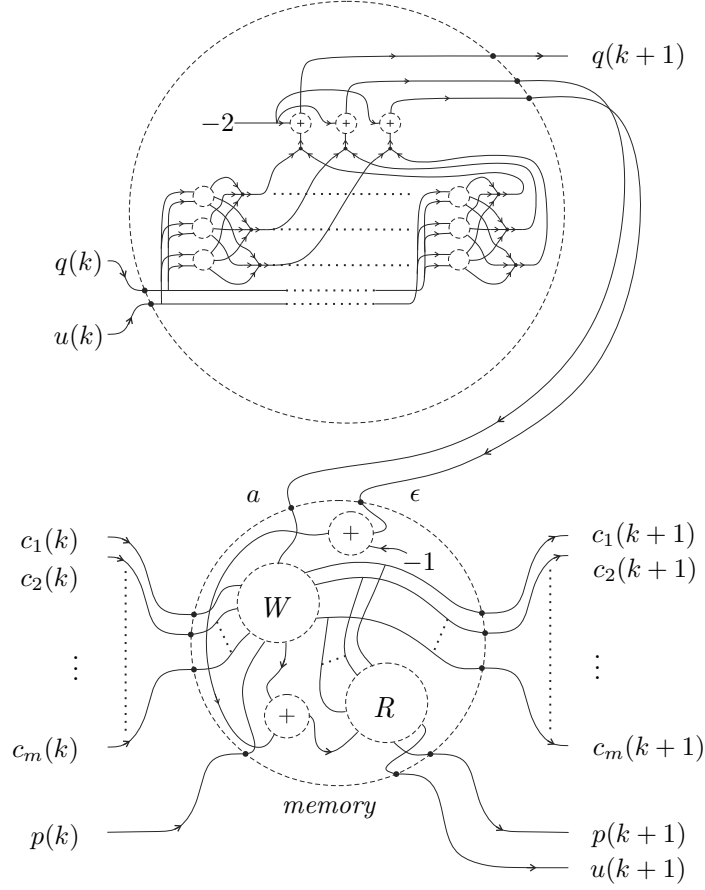


FIGURE 13. One-step computation of a Turing tangle.

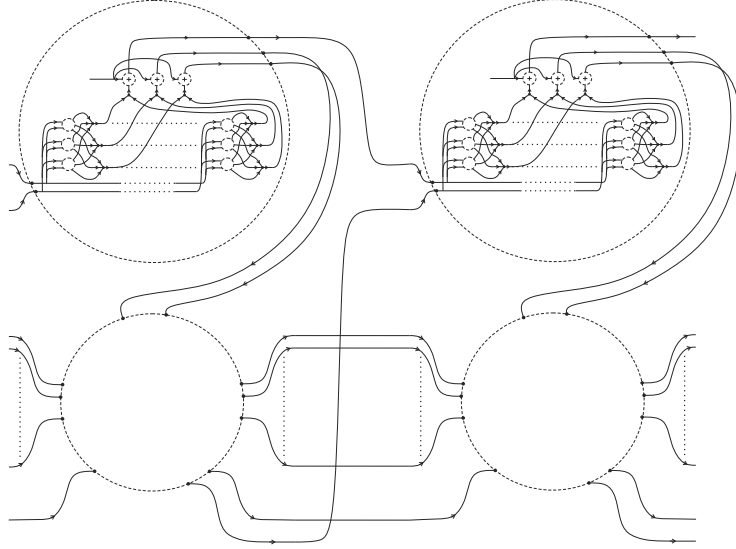


FIGURE 14. Iterative computation in a Turing tangle machine.

Consider an interaction at time t with agent V , one of whose patients is W . The realization w_{t+1} of W_{t+1} may equal either the belief of the agent v_t or the belief of the patient w_t . In other words, W either retains her belief or is ‘convinced’ by V to change her belief to that of V (we use female pronouns for the verifiers, who are all ‘Alices’). Whether or not V ‘succeeds in convincing W ’ depends on a message ξ_t from a *prover* Π with access to an *oracle*.

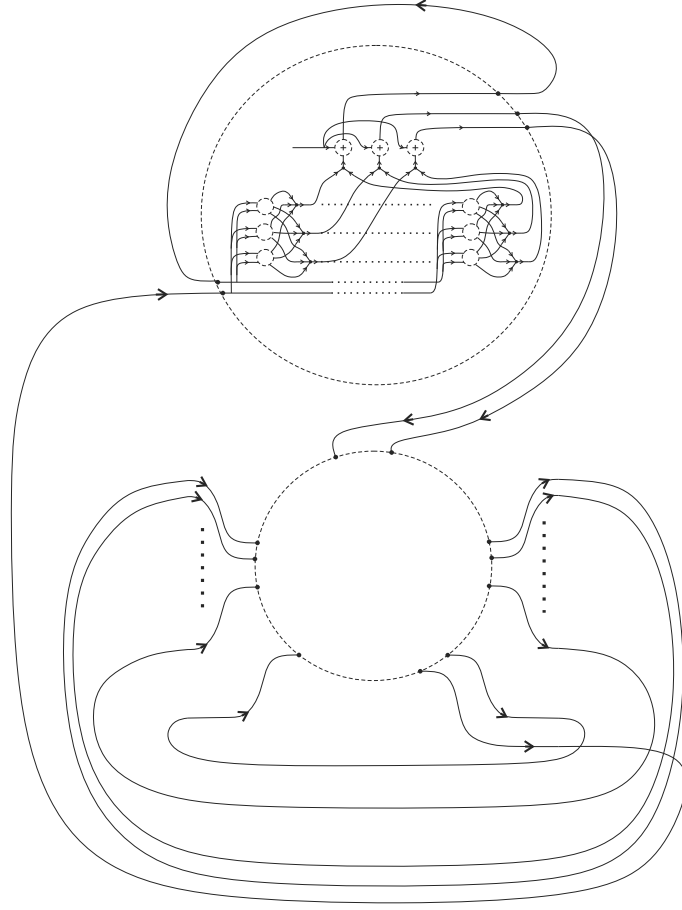


FIGURE 15. Closure of a Turing tangle machine in its halting state.

Only the belief of patients changes at an interaction. The agents and the verifiers who do not participate in the interaction do not change their beliefs, so in particular $v_{t+1} = v_t$ always.

There are three constants associated to the agent V at an interaction at time t : A *completeness parameter* c_V^t , a *soundness parameter* s_V^t with $0 < s_V^t < c_V^t \leq 1$, and a *deformation parameter* $\delta_V^t \in \mathbb{Q} \cap (0, 1)$. For simplicity, we will assume that these three parameters are the same for all agents in the network, and s_v^t, c_V^t, δ_V^t will be written s, c, δ correspondingly.

Our basic requirement for an interaction is that the following pair of inequalities be satisfied:

$$(25) \quad \begin{aligned} (\text{deformed completeness}) \quad & x \in L \longrightarrow \Pr(W_{t+1} = v_t \mid V_t = v_t) \geq c\delta; \\ (\text{deformed soundness}) \quad & x \notin L \longrightarrow \Pr(W_{t+1} = v_t \mid V_t = v_t) \leq s\delta. \end{aligned}$$

Remark 6. The deformed completeness and soundness, $c\delta$ and $s\delta$, may both be below $\frac{1}{2}$ or may both be above $\frac{1}{2}$ and bounded away from 1.

In the limit $\delta \rightarrow 1$, specific values of c and of s turn the pair of inequalities (25) into familiar pairs of inequalities in interactive proof theory [4]. For example, for $s = 2^{-|x|^a}$ and $c = 1 - 2^{-|x|^b}$, where $a, b > 0$, we obtain the completeness and soundness constraints of an IP verification.

6.2. Statistics of beliefs and interactions. When keeping track of the beliefs of many different verifiers at many different times, it is cumbersome to work directly with (25).

Instead, we introduce a shorthand to keep track of the belief of a verifier, both if $x \in L$ and also if $x \notin L$, in a single expression.

The *belief statistics* $|W_t\rangle$ of verifier W at time t is written:

$$(26) \quad |W_t\rangle \stackrel{\text{def}}{=} a |\text{True}\rangle + b |\text{False}\rangle ,$$

where $a \in [0, 1]$ denotes the *greatest lower bound* for the belief of W that $x \in L$ at time t conditioned on this belief indeed being true, and $b \in [0, 1]$ denotes the *greatest lower bound* for the belief of W that $x \notin L$ at time t conditioned on this opposite belief indeed being true. Note that $a + b$ need not equal 1. In particular:

$$(27) \quad \begin{aligned} x \in L &\longrightarrow a \leq \Pr(W_t = |\text{True}\rangle); \\ x \notin L &\longrightarrow b \leq \Pr(W_t = |\text{False}\rangle). \end{aligned}$$

An interaction between W and V at time t concludes either with W accepting the belief of V or with W sticking to her own belief. Denoting by h the probability (or more precisely a lower bound on it) of W switching to the belief of V in the next time-frame, the distribution of possible beliefs of W in the next time-frame is described by:

$$(28) \quad |W_{t+1}\rangle = |W_t\rangle^{V_t} \stackrel{\text{def}}{=} (1 - h) |W_t\rangle + h |V_t\rangle .$$

Remark 7. *Belief statistics written as in (26) facilitate calculations of probabilities across a network. This tool is used throughout the remainder of this note (some examples would be given shortly). Here we explain how (26) and (28) combine to give a compact way of representing two entirely different interactions, one assuming $x \in L$ and the other assuming $x \notin L$. This may be slightly confusing at first, so the reader's attention is called to this point.*

Owing to (28), the probabilities anywhere in the network at time $t > 0$ depend on the parameter h . We may do all calculations and treat it as a formal parameter. Having in mind that an interaction is ultimately a procedure terminating with the statistics in (25), the parameter h is set either to $c\delta$ or to $s\delta$ depending on whether or not x is in L . To verify that a network decides L we repeat the computation twice, first for the case where $x \in L$ and then for $x \notin L$. In the former case we will be interested only in the coefficient of $|\text{True}\rangle$ whereas in the latter case we will be interested only in the coefficient of $|\text{False}\rangle$.

Here is an illustrative calculation for a single interaction. Let $W_t = |\text{False}\rangle$ and $V_t = |\text{True}\rangle$. Invoke (28) using the completeness and soundness parameters in (25): first using $h = c\delta$ and then using $h = s\delta$. Hence,

$$|W_{t+1}\rangle = c\delta |\text{True}\rangle + (1 - s\delta) |\text{False}\rangle \longrightarrow \begin{cases} c\delta |\text{True}\rangle + (\dots) |\text{False}\rangle, & x \in L; \\ (\dots) |\text{True}\rangle + (1 - s\delta) |\text{False}\rangle, & x \notin L. \end{cases}$$

This interaction is said to decide L only if $c\delta > \frac{1}{2}$ and $1 - s\delta > \frac{1}{2}$.

6.3. Expressive power of a network: The class BraidIP. Verifiers in our framework are assumed to be implemented as probabilistic polynomial-time Turing machines whose beliefs are either internal states or are stored on tapes. Similarly, an interaction is a polynomial-time procedure. Consider now a crowd of verifiers V^1, V^2, \dots, V^μ whose initial beliefs at time $t = 0$ are $|V_0^1\rangle, |V_0^2\rangle, \dots, |V_0^\mu\rangle$. Allow them to interact at times $t = 0, 1, 2, \dots, \chi$, subject to parameters $0 < c < s \leq 1$ and $\delta \in \mathbb{Q} \cap (0, 1)$. We write M for this sequence of interactions. A language $L \subseteq \{0, 1\}^*$ is said to be *decided* by M if M contains a verifier V whose belief at time χ is $|V_\chi\rangle \stackrel{\text{def}}{=} a |\text{True}\rangle + b |\text{False}\rangle$, such that for a fixed constant $\kappa > 0$, we have:

$$(29) \quad \begin{aligned} x \in L &\longrightarrow a \geq \frac{1}{2} + |x|^{-\kappa}; \\ x \notin L &\longrightarrow b \geq \frac{1}{2} + |x|^{-\kappa}. \end{aligned}$$

This definition depends on the choice of $\kappa > 0$. The class *braided interactive polynomial time* (BraidIP) consists of those languages which are decidable for any fixed $\kappa > 0$ by some network M in time χ , polynomial in $|x|$. We denote this class $\text{BraidIP}\{\delta, \chi\}$ where χ is the number of interactions in M .

Remark 8. The definition of class BraidIP is similar in spirit to the class BPP. We will see below that it includes class IP. Letting (29) reflect the class PP (i.e. taking strict inequalities and right-hand constants equal to $\frac{1}{2}$) will result in networks that decide any $L \in \text{IPP}$.

6.4. Braid of beliefs. Our networks admit a convenient diagrammatic description. We represent an interaction as a wire cutting through other wires (see Figure 16). The overcrossing wire, which becomes slightly thickened in an interaction, carries the belief statistics of an agent whereas the undercrossing wires carry the belief statistics of her patients. An example of many concatenated interactions is given in Figure 17.

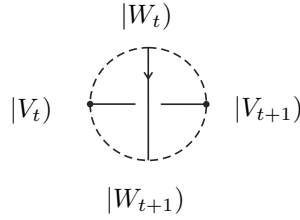


FIGURE 16. Diagrammatic representation of an interaction.

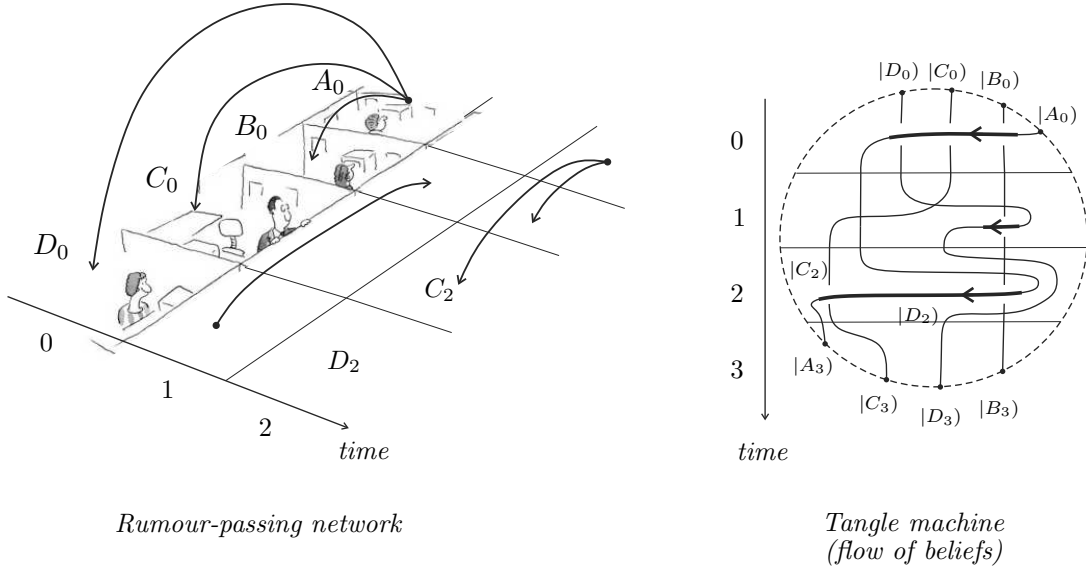


FIGURE 17. A rumour-passing network and its respective diagram.

The diagram representing the rumour passing network in Figure 17 is a *braid*, which is a special sort of *tangle*. Here, such diagrams represent the flow of beliefs within a network of interacting machines (verifiers).

When many patients pass under a single agent, we define this to imply that for each patient, the belief sampled from that patient is *independent* of the belief sampled from every other patient, and the belief sampled from the agent to update that patient's belief is independent of the belief sampled from the agent to update every other agent's belief. To say the same thing in a different way, multiple patients under the same agent are independent and unsynchronized during that time-frame. We will discuss this point further in Section 10.2.

6.5. An example. The capacity of a network to prove or disprove a claim is an emergent property. Out of a number of uncertain interactions, none of which prove the claim, the truth may eventually materialize. As an example, consider the two pairs of two consecutive interactions pictured in Figure 18. Both sequences involve three verifiers, designated X , Y and Z . Their initial beliefs are shown at the bottom.

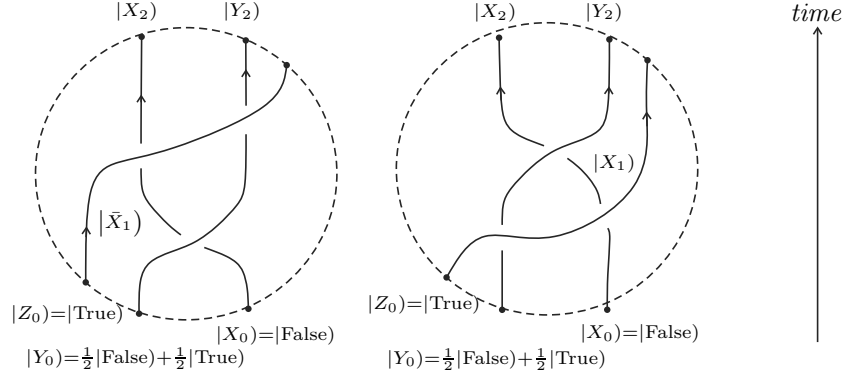


FIGURE 18. Equivalent networks of interactions.

Set the parameters to $s \stackrel{\text{def}}{=} \frac{1}{2}$, $c \stackrel{\text{def}}{=} 1$, and $\delta \stackrel{\text{def}}{=} \frac{1}{2}$. Allow the verifiers to interact in the left diagram. At time $t = 2$, beliefs X_0 and Y_0 of X and of Y have been updated to X_2 and to Y_2 (Z does not change his belief). The distributions are:

$$(30) \quad |X_2\rangle = \left(|X_0\rangle^{Y_0}\right)^{Z_0} \longrightarrow \begin{cases} \frac{3}{8} |\text{False}\rangle + \frac{5}{8} |\text{True}\rangle, & x \in L; \\ \frac{21}{32} |\text{False}\rangle + \frac{11}{32} |\text{True}\rangle, & x \notin L. \end{cases}$$

Hence,

$$(31) \quad \begin{aligned} |X_2\rangle &= \left(|X_0\rangle^{Y_0}\right)^{Z_0} = \frac{21}{32} |\text{False}\rangle + \frac{5}{8} |\text{True}\rangle, & (\text{left network}); \\ |X_2\rangle &= \left(|X_0\rangle^{Z_0}\right)^{(Y_0)^{Z_0}} = \frac{21}{32} |\text{False}\rangle + \frac{5}{8} |\text{True}\rangle, & (\text{right network}). \end{aligned}$$

Similarly,

$$(32) \quad |Y_2\rangle = |Y_1\rangle = |Y_0\rangle^{Z_0} = \frac{3}{8} |\text{False}\rangle + \frac{3}{4} |\text{True}\rangle.$$

From this we see that X decides correctly at time $\chi = 2$ with probability at least $\frac{5}{8}$ or $\frac{21}{32}$, depending on whether $x \in L$ or $x \notin L$. Both of these are greater than $\frac{1}{2}$, so the pair of inequalities 29, for a suitable $\kappa > 0$, a protocol underlied by the above interactions will succeed in deciding, at $|X_2\rangle$, whether or not $x \in L$.

Note again that

$$|Y_1\rangle = |Y_0\rangle^{Z_0} = h |Z_0\rangle + (1 - h) |Y_0\rangle,$$

and we evaluate with $h = \frac{1}{2}$ for the coefficient of $|\text{True}\rangle$ and with $h = \frac{1}{4}$ for the coefficient of $|\text{False}\rangle$. This is the same for all interactions in both diagrams.

Note that both diagrams in Figure 18 have the same *initial beliefs* $|X_0\rangle$, $|Y_0\rangle$, and $|Z_0\rangle$ and the same *terminal beliefs* $|X_2\rangle$, $|Y_2\rangle$, and $|Z_2\rangle$, and differ only in the belief of X at time $t = 1$. Thus, these two diagrams underlie *equivalent* deformed interactive proofs, each of which can uniquely be reconstructed from the other, which decide the same languages, but which differ at an intermediate step. This equivalence is the topic of Section 10.

7. DEFORMATION OF AN IP SYSTEM

In this section, we show how we may deform an IP system with any soundness parameters $0 < s < \frac{1}{2} < c \leq 1$, for any deformation parameter $\delta \in \mathbb{Q} \cap (0, 1)$. The completeness and soundness parameters of the deformed system will be $s\delta$ and $c\delta$ correspondingly. The deformation parameter δ serves to introduce noise between the prover and the verifiers. In the $\delta \rightarrow 1$ limit we recover IP, and the information obtained by a verifier at each interaction shrinks as $\delta \rightarrow 0$. But Theorem 4 proves that we can recover IP from BraidIP by concatenating many consecutive deformed interactions.

Before describing how IP may be deformed, we outline the major differences between a single interaction in IP and BraidIP:

Description	IP system	Deformed IP system
Participants	Verifier, Prover	Many verifiers (patient), Verifier (agent), Prover
Verifier 'state of mind'	Accept/Reject	Belief True/False
Conclusion	Verifier decides Accept/Reject	If the two verifiers do not agree then the patient may change her belief.
Completeness, Soundness	c, s	$c\delta, s\delta$

7.1. Two approaches to deform IP. We present two approaches to deform an IP protocol. The end result is the same, but the 'story' is different.

7.1.1. Agent and patient as a single verifier. We may think of a patient W and an agent V of an interaction at time t as representing different aspects of a single verifier. In this approach we conceive of W and V as being a single unit (W, V) . The verifier (W, V) transmits to the prover Π the belief of both W and V . We may imagine W and V as litigants in a court case, presenting their claims to the judge Π , where W is the defendant and V is the plaintiff. If both W and V make the same claim, then Π throws the case out (*i.e.* $W_{t+1} = w_t$ and $V_{t+1} = v_t$). On the other hand, if V disagrees with W , then (W, V) query the prover Π according to the original interactive protocol. If according to the original protocol, W 's claim should be accepted, then Π rules in W 's favour (*i.e.* $W_{t+1} = w_t$ and $V_{t+1} = v_t$). But if according to the original protocol W 's claim should be rejected and V 's claim should be accepted, then Π picks an integer uniformly at random between 1 and N . If the number Π picked is less than δN , then Π rules in favour of V (*i.e.* $W_{t+1} = v_t$ and $V_{t+1} = v_t$). Otherwise he rules in favour of W .

Perhaps δ represents a chosen standard of 'reasonable doubt'. Constants s and c perhaps represent constants associated with the mechanics of the courthouse procedure. Note that as $\delta \rightarrow 1$, a single interaction involving two verifiers with opposite beliefs recovers IP.

7.1.2. Verifiers communicating through a noisy channel. The following approach has an information-theoretic interpretation. Consider the prover Π as an information source, the agent verifier V as an encoder, and the patient verifier W as a decoder. The query information transmitted from W to Π is relayed via a perfect communication channel (*i.e.* there is no loss of information in this direction). The replies from Π are passed on to V who encodes them and transmits them back to W , this time through a noisy channel. This means that the prover replies emerge corrupted on W 's end, which consequently influences her decision.

Introducing a noisy channel into the formalism restricts the information obtained by the patient verifier from the prover. It tempting to state that the combination prover-agent-noisy channel behaves like a mendacious agent, in that the agent V decided whether

to prove the claim, the proof may yet emerge somewhere in the network depending on its topology.

The triple patients-agent-oracle brings to mind some basic models of reasoning and information transfer. Perhaps a patient is an entity whose beliefs reflect both prior knowledge and observations. The patient is exposed to a genuine phenomenon, which the patient has not seen before. The phenomenon, which is the metaphor for an oracle, is beyond the comprehension of the patient and hence a number of observations are collected in an attempt to reach a definitive conclusion. These observations, however, may be distorted by limitations of the patient measuring apparatus, or perhaps they contradict prevailing explanations and beliefs. In either cases observations contain, or otherwise introduce, uncertainty. Observations are the metaphor for agents. What the patient tries to accomplish underlies the Bayesian inference paradigm.

Here is another metaphor. A patient is a decoder, an oracle is an information source, and an agent is an encoder who relays the encoded oracle message through a noisy communication channel. Alternatively, an agent-patient pair is a verifier and the oracle is a prover who relays a message through a noisy communication channel. All metaphors reflect knowledge transfer subject to uncertainties.

7.2. Probabilistic theorem proving in networks. The goal of this section is to prove Theorem 4, repeated below for convenience.

Theorem 7. $\text{IP} \subseteq \text{BraidIP} \{\delta, \chi\}$ where:

$$(33) \quad I(c\delta) < \chi < \frac{1}{I(1-s\delta)},$$

with $I(p) \stackrel{\text{def}}{=} -p^{-1} \log p$. The growth rate of χ is $\mathcal{O}(\frac{1}{\delta})$ as $\delta \rightarrow 0$.

Proof of Theorem 4. We explicitly construct a configuration of interactions which decide a language L in IP. This configuration, which is illustrated in Figure 20 for the case $\chi = 4$ is a scaled up version of that in Figure 18. It involves $\chi + 1$ verifiers W and V^1, V^2, \dots, V^χ , and χ interactions. The parameters of all interactions are the same, and are c, s, δ .

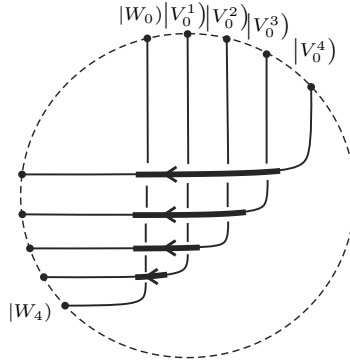


FIGURE 20. An interactive BraidIP theorem proving network with 5 verifiers W, V^1, V^2, V^3 , and V^4 , and 4 interactions.

Let $L \in \text{IP}$. The initial beliefs at time $t = 0$ are set to $|W_0\rangle \stackrel{\text{def}}{=} |\text{False}\rangle$ and

$$(34) \quad |V_0^i\rangle \stackrel{\text{def}}{=} \begin{cases} \frac{1}{2} |\text{False}\rangle + \frac{1}{2} |\text{True}\rangle, & 1 \leq i < \chi; \\ |\text{True}\rangle, & i = \chi. \end{cases}$$

Thus, at time zero there are two verifiers with opposite beliefs and $\chi - 1$ verifiers whose initial belief is that the claim $x \in L$ is 50% true and 50% false.

Calculating the output statistic $|W_\chi\rangle$ (which occurs at time χ) yields

$$(35) \quad |W_\chi\rangle \longrightarrow \begin{cases} (1 - c\delta)^\chi |\text{False}\rangle + [1 - c\delta - (1 - c\delta)^\chi] \left(\frac{1}{2} |\text{False}\rangle + \frac{1}{2} |\text{True}\rangle\right) + c\delta |\text{True}\rangle, & x \in L; \\ (1 - s\delta)^\chi |\text{False}\rangle + [1 - s\delta - (1 - s\delta)^\chi] \left(\frac{1}{2} |\text{False}\rangle + \frac{1}{2} |\text{True}\rangle\right) + s\delta |\text{True}\rangle, & x \notin L. \end{cases}$$

From (35) we see that the configuration in Figure 20 decides L if and only if:

$$(36) \quad \begin{aligned} x \in L &\longrightarrow (1 - c\delta)^\chi < c\delta; \\ x \notin L &\longrightarrow (1 - s\delta)^\chi > s\delta. \end{aligned}$$

From here we obtain the following bounds for χ :

$$(37) \quad \frac{\log(c\delta)}{\log(1 - c\delta)} < \chi < \frac{\log(s\delta)}{\log(1 - s\delta)}.$$

Equation 2 follows upon noting that $\log(1 - p) < -p$ for any $p \in (0, 1)$. Therefore:

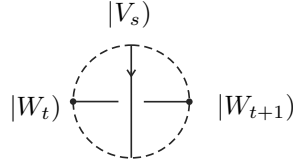
$$(38) \quad -\frac{1 - p}{\log(1 - p)} > \frac{\log p}{\log(1 - p)} > -\frac{\log p}{p}.$$

For χ within these bounds, the above configuration decides L . \square

Remark 9. Equation (2) tells us that χ has approximately the same growth rate in $|x|$ as $\frac{1}{\delta}$. By definition of BraidIP, χ 's growth rate is polynomial in the word length $|x|$, and so therefore δ is asymptotically bounded below by approximately one over a polynomial in $|x|$.

8. EFFICIENT IP STRATEGIES: TANGLED IP

8.1. The complexity class TangIP. We may extend class BraidIP by allowing each verifier to have its own 'local' time parameter, so that a patient belief W_t may interact with an agent belief V_s for $s \neq t$, and become updated to W_{t+1} .



We also allow verifiers to travel backwards or forwards in time and to update their previous or future beliefs, so that V_t may be updated by agent V_s to become V_{t+1} , where V_t and V_s are beliefs of one and the same verifier. Thus, each verifier may update their beliefs with past or future beliefs of itself (via feedback loops) or of other verifiers. We write M for a network of such concatenated interactions, subject to parameters $0 < c < s \leq 1$ and $\delta \in \mathbb{Q} \cap (0, 1)$. An example of such a network is given in Section 8.2.

A language $L \subseteq \{0, 1\}^*$ is said to be *decided* by M if M contains a verifier V whose belief at time χ is $|V_\chi\rangle \stackrel{\text{def}}{=} a |\text{True}\rangle + b |\text{False}\rangle$, such that for a fixed constant $\kappa > 0$ the inequalities (29) are satisfied.

The class *tangled interactive polynomial time* (TangIP) consists of those languages which are decidable for any fixed $\kappa > 0$ by some network M which contains χ interactions, where χ is polynomial in $|x|$. We denote this class $\text{TangIP}\{\delta, \chi\}$.

By Theorem 4 we know that

$$\text{IP} \subseteq \text{BraidIP} \subseteq \text{TangIP}.$$

We wonder about the connection between our classes BraidIP and TangIP and multi-prover IP (MIP) [11]. In particular, we wonder whether $\text{MIP} \subseteq \text{BraidIP}$ or $\text{MIP} \subseteq \text{TangIP}$, particularly if we allow different interactions to have different parameters (in this note all interactions are required to have the same parameters because that's all we need, but there is no obstruction to considering the more general case).

8.2. The Hopf–Chernoff configuration. Consider an IP system whose soundness s is nearly equal to its completeness c but for a small constant $\epsilon(|x|)$ that depends on the word length $|x|$, i.e. $c - s = \epsilon(|x|)$. As $\epsilon(|x|) \rightarrow 0$, the IP system becomes inefficient in the sense that it accepts every word with probability nearly c regardless of its membership in L . Yet we can still construct a deformed IP system that decides L . One may wonder how the number of interactions in such a system is affected by the decreasing gap $\epsilon(|x|)$.

The number of interactions in a network of the form given in Figure 20 is implicit in Theorem 4. Fix $\delta \in \mathbb{Q} \cap (0, 1)$ and note from Equation (2) that, as $\epsilon(|x|)$ decreases, the values bounding χ become nearly identical. But χ is an integer, so the two bounds must have an integer between them. In general, that means that the distance between them is at least 1. Therefore, the number of interactions grows as $\epsilon(|x|)$ decreases. We may need to take $\delta \rightarrow 0$ as $\epsilon(|x|) \rightarrow 0$. In fact it can be shown that in this case $\delta(|x|) = \mathcal{O}(\epsilon(|x|))$ which means that we require $\chi = \mathcal{O}(1/\epsilon(|x|))$ interactions.

Can fewer interactions decide L ? The configuration in Figure 21 decides L for any $\epsilon(|x|)$ using substantially less than $\mathcal{O}(1/\epsilon(|x|))$ interactions. This machine is a concatenation of a number of identical smaller configurations of interactions, denoted M_0, M_1, M_2, \dots . When concatenated to form a single configuration, we require approximately $\chi = \mathcal{O}(\log(1/\epsilon(|x|)))$ copies of M_0 to decide L (the precise argument is given below). If we were to trace its colours (probability generating functions) we would notice that it behaves much like a repetition of a binary random experiment (e.g. coin flipping), hence the magnitude of χ . We have named this configuration the *Hopf–Chernoff configuration* suggesting both to its structure and, to some extent, its functionality.

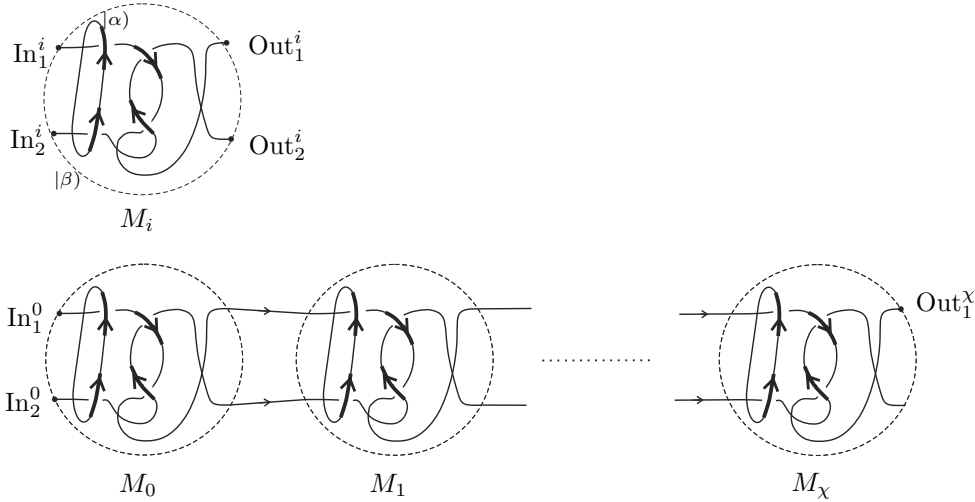


FIGURE 21. Hopf–Chernoff configuration(open version).

Theorem 8 (Hopf–Chernoff configuration). *Consider the configuration of interactions in Figure 21 which underlies a deformed IP system with completeness $c\delta$ and soundness $(c - \epsilon)\delta$, where $\epsilon > 0$. There exists a pair of beliefs, α and β , independent of any other belief in the machine, such that for any given set of initial beliefs In_j^0 the machine decides any $L \in \text{IP}$ using $\chi = \mathcal{O}(\log(1/\epsilon))$ submachines (and 4χ interactions). In particular, letting*

$$(39) \quad \begin{aligned} |\alpha\rangle &= \left(\frac{1}{4} + \frac{1}{12}\epsilon\delta\right) |\text{True}\rangle + \left(\frac{3}{4} - \frac{1}{12}\epsilon\delta\right) |\text{False}\rangle; \\ |\beta\rangle &= \left(1 - \frac{1}{2}c\delta + \frac{1}{12}\epsilon\delta\right) |\text{True}\rangle + \left(\frac{1}{2}c\delta - \frac{1}{12}\epsilon\delta\right) |\text{False}\rangle. \end{aligned}$$

yields

$$(40) \quad \text{Out}_1^\chi \longrightarrow \begin{cases} \left[\frac{1}{2} + \frac{1}{12}\epsilon\delta\right] |\text{True}\rangle + \left[\frac{1}{2} - \frac{1}{12}\epsilon\delta\right] |\text{False}\rangle, & x \in L; \\ \left[\frac{1}{2} - \frac{1}{12}\epsilon\delta\right] |\text{True}\rangle + \left[\frac{1}{2} + \frac{1}{12}\epsilon\delta\right] |\text{False}\rangle, & x \notin L. \end{cases}$$

namely, $\text{Out}_1^\chi = [\frac{1}{2} + \frac{1}{12}\epsilon\delta] |\text{True}) + [\frac{1}{2} + \frac{1}{12}\epsilon\delta] |\text{False})$.

Proof. Let us begin by writing down the relations between the outputs Out_j and inputs In_j of this machine. Note that

$$(41) \quad \text{Out}_1 = \left(\text{In}_1^{|\alpha\rangle} \right)^{\left(\text{In}_2^{|\beta\rangle} \right)}, \quad \text{Out}_2 = \left(\text{In}_2^{|\beta\rangle} \right)^{\left(\text{In}_1^{|\alpha\rangle} \right)}.$$

Explicitly writing (41) using the formal parameter h yields

$$(42) \quad \begin{bmatrix} \text{Out}_1^i \\ \text{Out}_2^i \end{bmatrix} = \underbrace{\begin{bmatrix} (1-h)^2 & h(1-h) \\ h(1-h) & (1-h)^2 \end{bmatrix}}_{\stackrel{\text{def}}{=} A(h)} \begin{bmatrix} \text{In}_1^i \\ \text{In}_2^i \end{bmatrix} + \underbrace{\begin{bmatrix} h(1-h) & h^2 \\ h^2 & h(1-h) \end{bmatrix}}_{\stackrel{\text{def}}{=} B(h)} \begin{bmatrix} |\alpha\rangle \\ |\beta\rangle \end{bmatrix}.$$

Letting $\text{In}_j^{i+1} = \text{Out}_j^i$, $j = 1, 2$, equation (42) underlies a linear dynamical system. It is easy to verify that the eigenvalues of the transition matrix $A(h)$ all are within the unit circle, i.e. $|\lambda(A(h))| < 1$ for any $h > 0$. That means that the system (42) reaches a steady-state as $i \rightarrow \infty$. The steady-state can be obtained as follows. Rewrite (42) as

$$(43) \quad \begin{bmatrix} \text{Out}_1 \\ \text{Out}_2 \end{bmatrix} = A(h) \begin{bmatrix} \text{Out}_1 \\ \text{Out}_2 \end{bmatrix} + B(h) \begin{bmatrix} |\alpha\rangle \\ |\beta\rangle \end{bmatrix},$$

and solve for Out_1 and Out_2 . Thus,

$$(44) \quad \begin{bmatrix} \text{Out}_1 \\ \text{Out}_2 \end{bmatrix} = (I - A(h))^{-1} B(h) \begin{bmatrix} |\alpha\rangle \\ |\beta\rangle \end{bmatrix} = \frac{1}{3-2h} \begin{bmatrix} 2(1-h)|\alpha\rangle + |\beta\rangle \\ |\alpha\rangle + 2(1-h)|\beta\rangle \end{bmatrix}.$$

Define

$$(45) \quad \begin{aligned} |\alpha\rangle &\stackrel{\text{def}}{=} a |\text{True}) + (1-a) |\text{False}); \\ |\beta\rangle &\stackrel{\text{def}}{=} b |\text{True}) + (1-b) |\text{False}). \end{aligned}$$

For the network to decide L we require the steady-state of Out_1 to satisfy

$$(46) \quad \text{Out}_1 \longrightarrow \begin{cases} (\frac{1}{2} + \sigma) |\text{True}) + (\frac{1}{2} - \sigma) |\text{False}), & x \in L; \\ (\frac{1}{2} - \sigma) |\text{True}) + (\frac{1}{2} + \sigma) |\text{False}), & x \notin L. \end{cases}$$

for some $\sigma > 0$. Using both (44) and (45) this requirement translates into the following set of equations

$$(47) \quad \begin{aligned} (3 - 2c\delta) (\frac{1}{2} + \sigma) &= 2(1 - c\delta)a + b, & x \in L; \\ (3 - 2(c - \epsilon)\delta) (\frac{1}{2} - \sigma) &= 2(1 - (c - \epsilon)\delta)a + b, & x \notin L. \end{aligned}$$

where the fact that $h = c\delta$ for $x \in L$ and $h = (c - \epsilon)\delta$ for $x \notin L$ has been used. Solving (47) for the coefficients a and b while assuming $\sigma = \frac{1}{12}\epsilon\delta$ yields (39). The underlying output probabilities in (40) are given by (46).

To complete the argument we need to show that the network converges within the stated number of iterations. It is sufficient to consider the case where the output probabilities (46) are attained to within the order $\mathcal{O}(\sigma) = \mathcal{O}(\epsilon)$. Growth rate of the system (42) is linear in $|\lambda_1(A(h))|^\chi$ where $\lambda_1(A(h))$ denotes the largest eigenvalue of $A(h)$. Simple calculation shows that $\lambda_1(A(h)) = 1 - h$ which yields $\chi = \mathcal{O}(\log(1/\epsilon))$. \square

The Hopf–Chernoff configuration is a recursive structure which is guaranteed to converge irrespective of its initial beliefs In_j^0 . In fact it represents a two-dimensional homogeneous irreducible Markov chain whose rate of convergence is $\mathcal{O}(2^{-\chi})$. Its stationary distribution, which depends on whether $x \in L$ or $x \notin L$, is given by (40). By virtue of its convergence properties we may just let it run forever (*i.e.* $\chi \rightarrow \infty$) knowing that it will eventually reach a stationary distribution not far from (40). For that reason we may as well substitute the open network in Figure 21 with its closed counterpart in Figure 22.

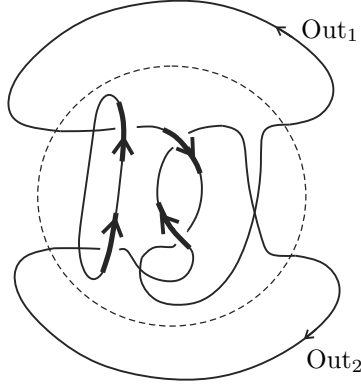


FIGURE 22. Hopf-Chernoff configuration (closed version).

9. PCP NETWORKS

In this section we specialize to non-adaptive 3-bit verifiers, to exhibit that tangle machines may exhibit better performance parameters than classical systems.

We deform the Håstad PCP verifier, which has $c = 1$ and $s \approx 0.75$. Suppose the two verifiers disagree, $v_t \neq w_t$, where $v_t, w_t \in \{|\text{True}\rangle, |\text{False}\rangle\}$. In this case the interaction proceeds as follows. The patient verifier W provides the addresses of three bits to Π . These bits are received by the agent verifier V which computes a certificate ξ_t , which is equal either to 1 meaning ‘accept’ or to -1 meaning ‘reject’. The agent then flips one out of the three bits with the following probabilities:

- $(\xi_t = 1) \wedge (v_t = |\text{True}\rangle) \rightarrow V$ flips a bit with probability $1 - \delta$.
- $(\xi_t = 1) \wedge (v_t = |\text{False}\rangle) \rightarrow V$ flips a bit with probability δ .
- $(\xi_t = -1) \wedge (v_t = |\text{True}\rangle) \rightarrow V$ flips no bit.
- $(\xi_t = -1) \wedge (v_t = |\text{False}\rangle) \rightarrow V$ flips a bit.

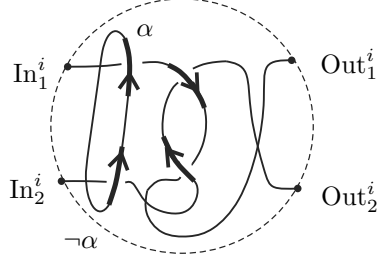
The corrupted set of bits is then sent back to W who computes her own certificate. This protocol realizes the communication channel in Figure 19.

9.1. A better-than-classical PCP verifier. In this section, we construct a tangle machine whose interactions are deformed Håstad verifiers, which has perfect accuracy and a completeness of $\frac{2}{3} + \sigma \approx 0.667$. This is worse than the conjectured bound of 0.625, but better than the best-known classical non-adaptive 3-bit PCP protocol, whose soundness is only around 0.741. Thus, our machine behaves like a single very good verifier.

Our machine makes use of the Hopf-Chernoff configuration in Figure 21.

- (1) Choose input beliefs In_j^0 , $j = 1, 2$, arbitrarily from $\{|\text{True}\rangle, |\text{False}\rangle\}$. Assume $c = 1$ and fix δ .
- (2) Let α be a Bernoulli distribution with parameter $\frac{1}{2}$. Draw a belief from α for the top agent, and set the bottom agent to the negation of that belief. We colour the bottom agent as $\neg\alpha$, which equals α as a distribution, to diagrammatically signify what we are doing.
- (3) Do the following for $i = 1, \dots, \chi$, where $\chi = \mathcal{O}(1)$:
 - Using the underlying deformed PCP verifier, perform the four interactions of the Hopf-Chernoff configuration to propagate the beliefs of the two verifiers

from In_j^i to Out_j^i according to the diagram below.



- Set $\text{In}_j^i = \text{Out}_j^{i-1}$, $j = 1, 2$.

- (4) If the patient belief in the output $\text{Out}_1^x = \neg\alpha$ then return $|\text{True})$, otherwise return $|\text{False})$.

Theorem 9. *The Hopf-Chernoff machine approaches perfect completeness and soundness at most $\frac{1}{3-2s}$ as $\delta \rightarrow 1$. In particular, if we put deformed Håstad verifiers at interactions, its soundness is at most $\frac{2}{3}$.*

Proof.

Completeness: Assume that $x \in L$ and note that as $\delta \rightarrow 1$, so does $h = c\delta \rightarrow 1$. In the limit where $h = 1$ note that by (37) the Hopf-Chernoff swaps the beliefs α and $\neg\alpha$ such that always $\text{Out}_1 = \neg\alpha$ and $\text{Out}_2 = \alpha$. Thus step (iv) of the algorithm concludes with $|\text{True})$.

Soundness: The soundness of the algorithm bounds the probability that $\text{Out}_1 = \neg\alpha$ in case where $x \notin L$. This probability is given by

$$(48) \quad \Pr(\text{Out}_1 = \neg\alpha) = \Pr(\text{Out}_1 = |\text{True}) \mid \alpha = |\text{False})) \Pr(\alpha = |\text{False})) \\ + \Pr(\text{Out}_1 = |\text{False}) \mid \alpha = |\text{True})) \Pr(\alpha = |\text{True})).$$

Although not truly essential, the algorithm assumes $\Pr(\alpha = |\text{True})) = \frac{1}{2}$. The conditional probabilities above can be bounded using (37) as follows. Take $h = s\delta \rightarrow s$ and assume that $|\alpha) = |\text{False})$. In this case (37) implies:

$$(49) \quad \Pr(\text{Out}_1 = |\text{True}) \mid \alpha = |\text{False})) \leq \frac{1}{3-2s}.$$

On the other hand, letting $|\alpha) = |\text{True})$, the same equation reads:

$$(50) \quad \Pr(\text{Out}_1 = |\text{False}) \mid \alpha = |\text{True})) \leq \frac{1}{3-2s}.$$

This follows from the fact that the algorithm decides $x \in L$ if $\text{Out}_1 = \neg\alpha$ irrespective of the beliefs themselves. For that reason these equations coincide, though for different values of α and Out_1 . Both describe a failure of the algorithm to decide $x \notin L$. The theorem now follows from (48), (49) and (50). \square

10. LOW-DIMENSIONAL TOPOLOGY AND BISIMULATION

Definition 10. *A tangle machines M and M' which each come equipped with a distinguished set of input and output registers are bisimilar if any computation that can be carried out on M can be carried out on M' and vice versa.*

Because computations are defined only with respect to the pre-chosen sets of input and of output registers, Definition 10 encapsulates what may be thought of as a *weak* notion of bisimulation (no requirement is made on ‘silent’ or ‘internal’ interactions).

In Section 10.1 we formulate a set of local moves, such that any two machines related by these local moves are bisimilar. In Section 10.2 we discuss a feature of our formalism, that is the ‘unsplittability’ of our agent registers. In Section 10.3 we suggest an application

of machine equivalence to define a notion of *zero knowledge* for tangle machines and to utilize it to construct TangIP machines which are ‘more secure’ in a specific sense. We give an example in Section 10.4. Finally, in Section 10.5, we extend our notion of machine equivalence to machines which may have wyes.

10.1. Equivalence. The key property of tangle machines is that they admit a local notion of equivalence [16]. Two (quandle coloured, without wyes) tangle machines are *equivalent* if they are related by a finite sequence of the moves in Figures 23 and 24. It is forbidden for these moves to involve input and output registers of a computation.

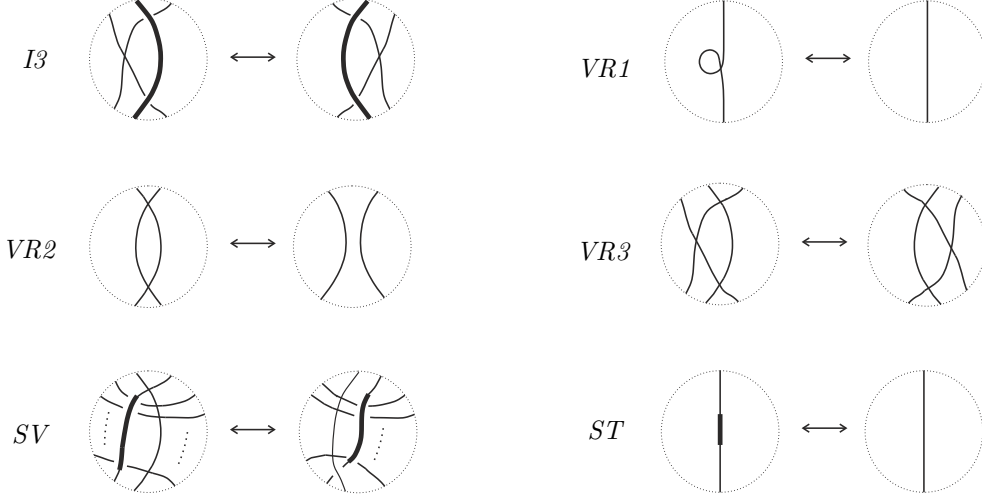


FIGURE 23. Cosmetic moves for machines. Directions are not indicated, meaning that the moves are valid for any directions, and the same for colourings.

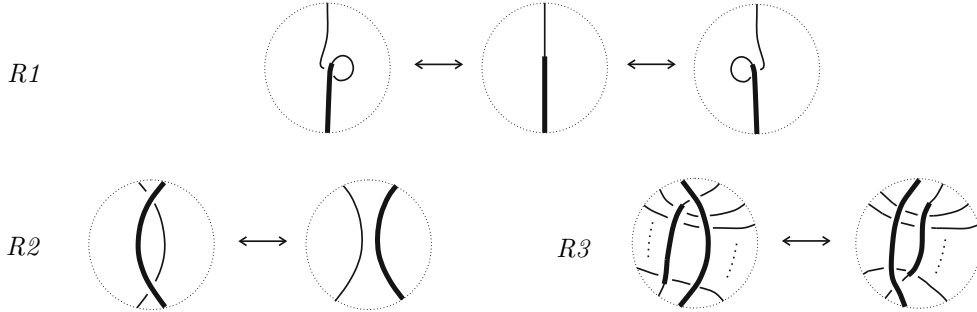


FIGURE 24. Reidemeister moves for machines, valid for any directions of the agents. It is forbidden for these moves to involve input and output registers of a computation.

Two machines related by the local moves in Figure 23 carry out identical computations, and it follows from the construction of an interaction that two machines related by R1 differ only by a trivial computation at which ‘nothing happens’. Thus, the interesting moves for us are R2 and R3 in Figure 24, which we will say more about later on.

Remark 10. First note that, for R2 to make sense, all participating colours must be defined. This requirement is non-trivial for a machine coloured by a quandle.

Remark 11. For a machine coloured by a quagma, the R3 move is replaced by the following

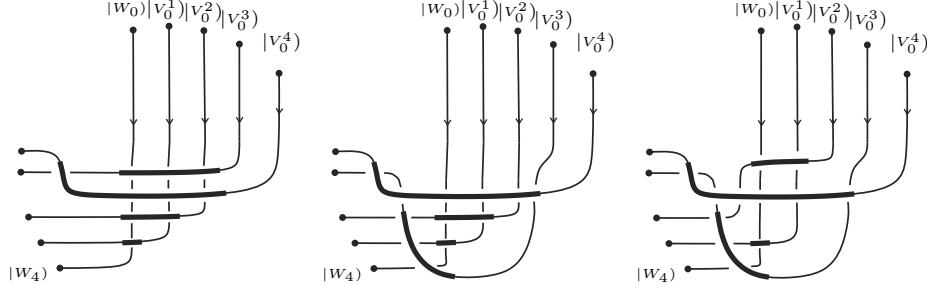


FIGURE 25. Equivalent prover strategies for the machine in Figure 20.

(51)

for all $\triangleright, \blacktriangleright \in B$ satisfying $(x \triangleright y) \blacktriangleright z = (x \blacktriangleright z) \triangleright (y \blacktriangleright z)$ for all $x, y, z \in Q$.

If we choose input and output registers to be machine endpoints, then equivalent machines have identical initial and terminal beliefs which implies that both machines have the same computational power in terms of deciding a language. Nevertheless, the local behaviour of equivalent may be different, in that the colours of intermediate interactions in between the same initial and terminal statistics may be different in equivalent machines. As in the earlier example in Figure 18, equivalent machines may two different prover strategies arriving at the same proof.

To expand that example, Figure 25 features several equivalent prover strategies for the machine in Figure 20 all which are obtained by application of R3 moves.

10.2. The single agent in R2 and R3. In this section we discuss the single agent which acts on numerous patients and cannot be split. Such an agent features in Moves R2 and R3, and distinguishes our approach *e.g.* from w-tangles [9].

The R2 move tells us that computations are reversible, in the sense that any operation $\triangleright \in B$ has an inverse operation $\triangleleft \in B$ such that no information is computed from $(x \triangleright y) \triangleleft y$ for any $x, y \in Q$. Because we are working not only with colours but with realizations of belief statistics, we are saying more than just $(x \triangleright y) \triangleleft y = x$. We require that there be zero knowledge gain about realizations of $(x \triangleright y) \triangleleft y$ from a realization of x .

(52)

Our formalism features agents that act on multiple patients. These actions are independent by definition. Conversely, as we saw in Section 8.2, different agents may cooperate, for example by coordinating their realizations to be the same or to be opposed to one another.

We do not impose the following a-priori reasonable generalization of R2.

(53)

One reason that we do not impose (53) can be seen by considering the example in which the two agents in the machine on the left-hand side adopt the strategy of always offering the same realization. If the realization of the patient and of the agent coincide, we can compute the realizations of both other patients. If not then we cannot. Thus we can compute the colours of the remaining patients in (53) for some realizations but not for others. This behaviour is not shared by the machine on the right hand side, in which colours the realizations of patients can never be computed unless they are already given. If the choice of realization is independent for both patients, *i.e.* if there is only a single interaction, as in the case of ‘honest’ R2, there is no such phenomenon, and no choice of realizations for input registers is distinguished from any other. Note also that (53) represents two distinct computations, each of which can be considered separately and each of which is non-trivial, which is not true for the right-hand side of the ‘honest’ R2.

For the same reason, we do not impose the following ‘fake R3 move’:

(54)

10.3. Zero knowledge. The theory of IP features the notion of a zero-knowledge proof [22, 21]. In a zero-knowledge proof, the information that may be gained by the verifier in the course of her interactions with the prover are restricted. This is useful when the verifier may not always be trustworthy. The definition makes use of a simulator which is an arbitrary feasible algorithm that is able to reproduce the transcript of such an interaction without ever interacting with the prover.

We suggest the following definition as a TangIP analogue to the notion of zero knowledge.

Definition 11 (Zero knowledge tangle machine). *A tangle machine M that decides a language $L \in \text{TangIP}$ is said to be zero knowledge if the following is satisfied.*

- (1) *There are no intermediate interactions in M that decides L .*
- (2) *There exists an equivalent machine M' which decides L at one of its intermediate interactions.*

Remark 12. *The idea of zero knowledge tangled IP parallels the authors’ model of fault-tolerant information fusion networks, except that there we wanted intermediate registers to ‘know as much as possible’ whereas here we want them to ‘know as little as possible’ [15].*

As a generic example, consider machines M' and M in Figure 26. Both share the same initial and terminal belief statistics. The explicit structure of the machines is mostly irrelevant except that they both contain a submachine S which we graphically represent by a blank disk, with the property that M , M' , and some of S ’s terminal statistics $|Y_i\rangle$ decide L . In M , the verifier Z is an agent to all initial states of S and the resulting beliefs from this interaction are $|X_i\rangle$, $i = 1, 2, \dots$. In M' the same verifier is an agent to the

terminal states of S and the resulting beliefs from this interaction are characterized by $|Y_i\rangle$.

That M is zero-knowledge implies the proof should not appear somewhere within it. Assuming none of the In_i 's decide L , and neither do any intermediate belief states of S , this requirement implies that none of the $|X_i\rangle = (\text{In}_i)^{|Z\rangle}$ decide L . On the other hand, the machine M' shows us that an interaction between the terminal states of S , some of which decide L , with the agent Z are able to produce the proof. That is, some of $\text{Out}_i = |Y_i\rangle^{|Z\rangle}$ decide L . These requirements completely characterize the belief distribution $|Z\rangle$. Perhaps unsurprisingly, it turns out that $|Z\rangle = \frac{1}{2}|\text{True}\rangle + \frac{1}{2}|\text{False}\rangle$.

Ideally we would require that S reproduces the proof as if it was produced by M itself. This requirement translates into

$$(55) \quad |Y_i\rangle = \text{Out}_i,$$

for any Out_i that decides L . As both sides of (55) depend on the deformation parameter δ , this equation may be used to determine δ such that M is zero-knowledge. Below we give an example.

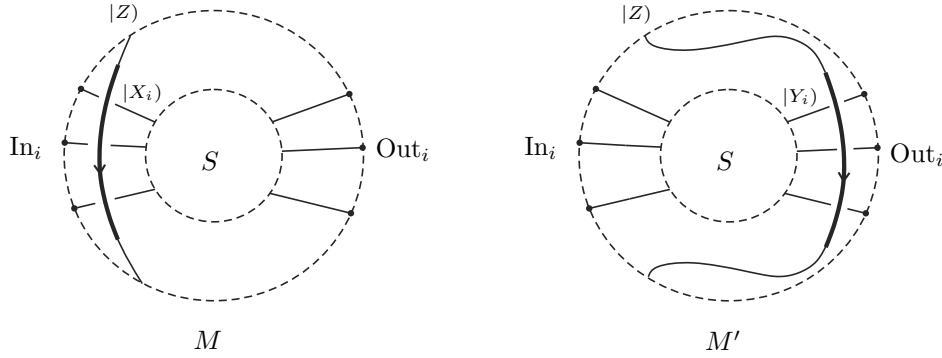


FIGURE 26. Two equivalent machines. The machine M is zero-knowledge. The proper submachine S determines L .

10.4. Example. Consider the two machines in Figure 27. Assume they both employ a deformed IP system whose completeness and soundness are δ and $\frac{1}{2}\delta$. Let $|Z\rangle = \frac{1}{2}|\text{False}\rangle + \frac{1}{2}|\text{True}\rangle$ and let us first see what the value of δ is for the machine to decide L . The output $|X_2\rangle$ of either machines is given by

$$(56) \quad |X_2\rangle \longrightarrow \begin{cases} [(1-\delta)^2 + \frac{1}{2}\delta] |\text{False}\rangle + [\delta(1-\delta) + \frac{1}{2}\delta] |\text{True}\rangle, & x \in L; \\ [(1-\frac{1}{2}\delta)^2 + \frac{1}{4}\delta] |\text{False}\rangle + [\frac{1}{2}\delta(1-\frac{1}{2}\delta) + \frac{1}{4}\delta] |\text{True}\rangle, & x \notin L. \end{cases}$$

from which we conclude that $\delta > \frac{1}{2}$. The machine on the right in this figure is zero-knowledge because $|X_1\rangle$ does not decide L :

$$(57) \quad |X_1\rangle \longrightarrow \begin{cases} [1 - \frac{1}{2}\delta] |\text{False}\rangle + \frac{1}{2}\delta |\text{True}\rangle, & x \in L; \\ [1 - \frac{1}{4}\delta] |\text{False}\rangle + \frac{1}{4}\delta |\text{True}\rangle, & x \notin L. \end{cases}$$

and on the other hand the submachine inside the small disk on the left decides L :

$$(58) \quad |\bar{X}_1\rangle \longrightarrow \begin{cases} [1 - \delta] |\text{False}\rangle + \delta |\text{True}\rangle, & x \in L; \\ [1 - \frac{1}{2}\delta] |\text{False}\rangle + \frac{1}{2}\delta |\text{True}\rangle, & x \notin L. \end{cases}$$

If we further restrict the value of δ so as to satisfy (55), namely,

$$(59) \quad |\bar{X}_1\rangle = |X\rangle_2 \longrightarrow \delta = \delta(1-\delta) + \frac{1}{2}\delta,$$

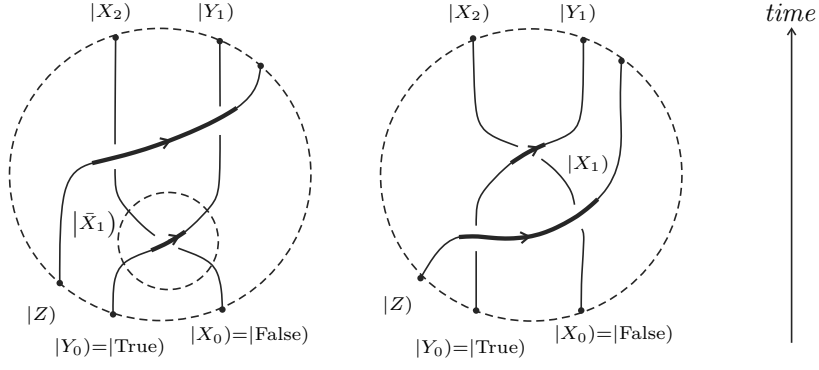


FIGURE 27. Example of a zero-knowledge machine.

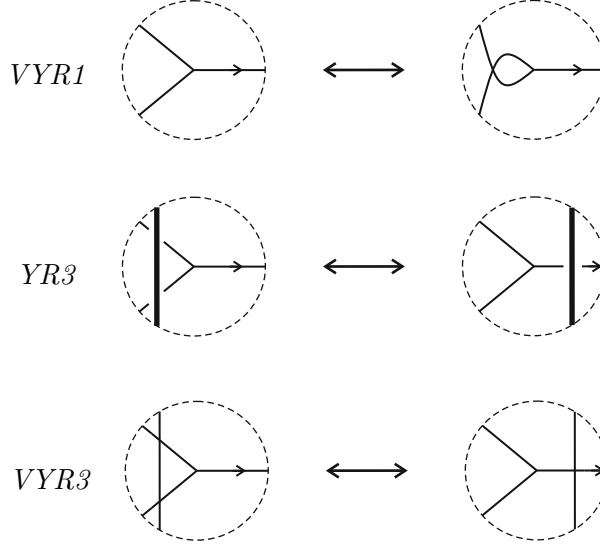


FIGURE 28. Local moves for wyes. Note that YR3 may reverse the label on the wye (max to min or vice versa), depending on what the colours are.

we obtain $\delta = \frac{1}{2}$ which obviously contradicts the basic requirement of deciding L . If we slightly relax this condition to allow a small discrepancy between the underlying distributions then we may take $\delta = \frac{1}{2} + \kappa(x)$ where $\kappa(x)$ is a statistical distance which potentially depends on x .

10.5. Equivalence for machines with wyes. Machines coloured by quagmas as machines with wyes also have a notion of equivalence, giving them a certain flexibility as a diagrammatic language. Two trivalent machines are *equivalent* if they are related by a finite sequence of moves in Figure 23, 24, and 28.

11. CONCLUSIONS

In this paper we have suggested a Turing-complete diagrammatic model of computation, in which computers are drawn as tangles of decorated coloured strings. With bounded resources, our ‘tangle machines’ can decide any language in complexity IP , sometimes more efficiently than known classical single-verifier models. Our machines admit a notion of equivalence that they inherit from low-dimensional topology, with equivalent machines representing bisimilar computations. Topological invariants of our machines would be characteristic quantities for these computations which are invariant over bisimilarity classes.

REFERENCES

- [1] Abramsky, S. No-cloning in categorical quantum mechanics. In *Semantic Techniques in Quantum Computation*, (I. Mackie & S. Gay Ed.), Cambridge University Press, 2010; pp. 1–28. [arXiv:0910.2401](#)
- [2] Abramsky S., & Coecke, B. 2009 Categorical quantum mechanics. In *Handbook of Quantum Logic and Quantum Structures*, Vol. 2, 261–323. [arXiv:0808.1023](#)
- [3] Alagic, G., Jeffery, S., & Jordan, S. Circuit Obfuscation Using Braids. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2014)* (eds. S.T. Flammia & A.W. Harrow), Vol. 27, pp. 141–160. [arXiv:1212.6458](#)
- [4] Arora, S., & Barak, B. 2009 Computational complexity: A modern approach. Cambridge University Press.
- [5] Arora, S., Lund, C., Motwani, R., Sudan, M., & Szegedy, M. 1998 Proof verification and hardness of approximation problems. *Journal of the ACM* **45**(3), 501–555.
- [6] Arora, S. & Safra, S. 1998 Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM* **45**(1), 70–122.
- [7] Babai, L., Fortnow, L., & Lund, C. 1991 Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, **1**, 3–40.
- [8] Baez, J., & Stay, M. 2011 Physics, topology, logic and computation: A Rosetta stone. In *New Structures for Physics*, Lecture Notes in Phys. **813**, 95–172. [arXiv:0903.0340](#)
- [9] Bar-Natan, D., & Dancso, S. 2013 Finite type invariants of w-knotted objects I: W-knots and the Alexander polynomial. Manuscript submitted for publication. [arXiv:1405.1956](#)
- [10] Barrington, D.A. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 . *J. Comput. System Sci.* **1989**, 38(1), 150–164.
- [11] Ben-Or, M., Goldwasser, S., Kilian, J., & Wigderson, A. 1988 Multi prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th ACM Symposium on Theory of Computing*, 113–121.
- [12] Buliga, M. 2011 Braided spaces with dilations and sub-riemannian symmetric spaces. In *Geometry. Exploratory Workshop on Differential Geometry and its Applications*, (D. Andrica & S. Moroianu Ed.), Cluj-Napoca 21–35. [arXiv:1005.5031](#)
- [13] Buliga, M. 2011 Computing with space: A tangle formalism for chora and difference. Preprint. [arXiv:1103.6007](#)
- [14] Buliga, M., & Kauffman, L. 2013 GLC actors, artificial chemical connectomes, topological issues and knots. In *ALIFE 14: Proceedings of the Fourteenth International Conference on the Synthesis and Simulation of Living Systems*, 490–497. [arXiv:1312.4333](#)
- [15] Carmi, A.Y. & Moskovich, D. 2014 Low dimensional topology of information fusion. In *BICT14: Proceedings of the 8th International Conference on Bio-inspired Information and Communications Technologies*, ACM/EAI, 251–258. [arXiv:1409.5505](#)
- [16] Carmi, A.Y. & Moskovich, D. 2015 Tangle machines. *Proc. R. Soc. A* **2015**, 471, 20150111. [arXiv:1408.2862](#)
- [17] Churchill, F.B. William Johannsen and the genotype concept *J. Hist. Biol.* **1974**, 7, 5–30.
- [18] Clark, D., Morrison, S. & Walker, K. 2009 Fixing the functoriality of Khovanov homology. *Geom. Topol.* **13**(3), 1499–1582.
- [19] Elhamdadi, M. 2014 Distributivity in Quandles and Quasigroups. In *Algebra, Geometry and Mathematical Physics*, Springer Berlin Heidelberg, 325–340. [arXiv:1209.6518](#)
- [20] Fredkin, E. & and Toffoli, T. Conservative logic. *Int. J. Theor. Phys.* **1982**, 21(3/4), 219–253.

- [21] Goldreich, O. 2010 A short tutorial of zero-knowledge. Unpublished. <http://www.wisdom.weizmann.ac.il/oded/zk-tut02.html>
- [22] Goldwasser, S., Micali, S., & Rackoff, C. 1989 The Knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, **18**(1), 186–208.
- [23] Håstad, J. 1997 Some optimal inapproximability results. *Journal of the ACM*, **48**(4), 798–859.
- [24] Hopcroft, J.E., Motwani, R., & Ullman, J.D. 2001 *Introduction to Automata Theory, Languages, and Computation*. (2nd ed.), Reading Mass: AddisonWesley.
- [25] Ishii, A., Iwakiri, M., Jang, Y., & Oshiro, K. 2013 A G -family of quandles and handlebody-knots. *Illinois J. Math.*, **57**, 817–838. [arXiv:1205.1855](#)
- [26] Johannsen, W. The genotype conception of heredity. *Am. Nat.* **1911**, 45(531), 129–159.
- [27] Joyce, D. 1982 A classifying invariant of knots: The knot quandle. *J. Pure Appl. Algebra* **23**, 37–65.
- [28] Kauffman, L.H. 1994 Knot automata. In *Twenty-Fourth International Symposium on Multiple-Valued Logic, Conference Proceedings*, 328–333.
- [29] Kauffman, L.H. 1995 Knot logic. In *Knots and Applications*, Series of Knots and Everything **6**, World Scientific Publications, 1–110.
- [30] Kauffman, L.H. 1999 Virtual knot theory. *Europ. J. Combinatorics* **20**(7), 663–690. [arXiv:math/9811028](#)
- [31] Kauffman, L.H. & Lomonaco Jr, S.J. 2004 Braiding operators are universal quantum gates. *New J. Phys.*, **6**(1), 134. [arXiv:quant-ph/0401090](#)
- [32] Khot, S., & Saket, R. 2006 A 3-query non-adaptive PCP with perfect completeness. In *Proceedings of the 21st IEEE Conference on Computational Complexity*, 159–169.
- [33] Kitaev, A.Yu. Fault-tolerant quantum computation by anyons. *Ann. Phys.* (2003), **303**, 2–30. [arXiv:quant-ph/9707021](#)
- [34] Krohn, K., Maurer, W.D., & Rhodes, J. Realizing complex boolean functions with simple groups. *Inform. Control* **1966**, 9(2), 190–195.
- [35] Meredith, L.G. & Snyder, D.F. 2010 Knots as processes: A new kind of invariant. Preprint. [arXiv:1009.2107](#)
- [36] Mochon, C. Anyons from nonsolvable finite groups are sufficient for universal quantum computation. *Phys. Rev. A* **2003**, 67(2), 022315. [arXiv:quant-ph/0206128](#)
- [37] Moshkovitz, D., & Raz, R. 2010 Two-query PCP with subconstant error. *Journal of the ACM* **57**(5), 29.
- [38] Nayak, C., Simon, S.H., Stern, A., Freedman, M., & Sarma, S.D. 2008 Non-Abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, **80**(3), 1083–1159. [arXiv:0707.1889](#)
- [39] Ogburn, R.W. & Preskill, J. Topological quantum computation. In *Quantum Computing and Quantum Communications*, Lecture Notes in Comput. Sci. **1509**, 1999; pp. 341–356. Springer.
- [40] Peirce, C.S., 1880 On the algebra of logic. *Amer. J. Math.*, **3** 15–57.
- [41] Przytycki, J.H. 2011 Distributivity versus associativity in the homology theory of algebraic structures. *Demonstr. Math.*, **44**(4), 823–869. [arXiv:1109.4850](#)
- [42] Roscoe, A.W. 1990 Consistency in distributed databases. *Oxford University Computing Laboratory Technical Monograph* **PRG-87**.
- [43] Shamir, A. 1992 $IP = PSPACE$. *Journal of the ACM*, **39**(4), 869–877.
- [44] Surowiecki, J. 2005 *The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations*. Random House LLC.
- [45] Turing, A.M. 1937 *On computable numbers, with an application to the Entscheidungsproblem*. P. Lond. Math. Soc. Ser. 2 **42**, 230–265. (and Turing, A.M. 1938 *On computable numbers, with an application to the Entscheidungsproblem: A correction*. P. Lond. Math. Soc. Ser. 2 **43**, 544–546.

- [46] Vicary, J. 2012 Higher Semantics for Quantum Protocols. In *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science*, 606–615. [arXiv:1207.4563](#)
- [47] Zwick, U. 1998 Approximation algorithms for constraint satisfaction problems involving at most three variables per constraint. In *Proceedings of the 9th ACM-SIAM Symposium on Discrete Algorithms*, 201–210.

FACULTY OF ENGINEERING SCIENCES &, CENTER FOR QUANTUM INFORMATION AND TECHNOLOGY,
BEN-GURION UNIVERSITY OF THE NEGEV, BEER-SHEVA 8410501, ISRAEL